IndustrialPro® 6000 Routers

RAM® 6000 Series Cellular RTUs

RAM® 9000 Cellular RTUs

Software User Guide

Version 3.17/4.17

www.redlion.net

Chapter 1 Accessing the Web User Interface 4
1.1 Connect PC to Red Lion Router 4
1.2 Setup PC IP Address 5
1.2.1 Open the Control Panel 5
1.2.2 Access Network and Settings 5
1.2.3 Access Network Connection Settings 6
1.2.4 Access Local Area Connection 6
1.2.5 Open Properties 7
1.2.6 Access Internet Protocol Properties 7
1.3 Access Red Lion Web Server 11
1.3.1 Red Lion Router Login Instructions 11
1.3.2 SSH, Telnet, Serial RS-232 Connections to Red Lion Routers 12
Chapter 2 Cellular Connections 13
2.1 Cellular Configuration 13
2.1.1 Cellular Interface Configuration 14
2.1.2 Set the User Name, Password and APN 14
2.1.3 Provisioning 15
2.1.4 Verify Cellular Connectivity 15
2.1.5 Cellular Connectivity Troubleshooting 16
Chapter 3 Web User Interface 20
3.1 Web User Interface Introduction 20
3.1.1 Organization 20
3.2 Status Tab 21
3.2.1 Summary 21
3.2.2 Network 24
3.2.3 Diagnostics 27
3.2.4 Syslog 31
3.2.5 Gather Stats 32
3.3 Admin Tab 34
3.3.1 Access Settings 34
3.3.2 System Time 35
3.3.3 Certificate Manager 37
3.3.4 Firmware Update 39
3.4 Network Tab 44
3.4.1 Cellular Connection 44
3.4.2 Interfaces 49
3.4.3 Firewall 60
3.4.4 Tunneling 74
3.4.5 DNS Settings 83
3.4.6 Static Routes 85
3.4.7 TCP Global Settings 86
3.5 Services Tab 88
3.5.1 DHCP Server 88
3.5.2 DHCP Relay 91
3.5.3 Dynamic DNS 93

3.5.4 SN Proxy Settings 95
3.5.5 SixView Manager 96
3.5.6 GPS Settings 98
3.5.7 SSH/TELNET Server 101
3.5.8 SSL Connections 102
3.5.9 SNMP Agent 108
3.5.10 Ping Alive 109
3.5.11 Serial IP 110
3.6 Automation Tab 114
3.6.1 Local Station 115
3.6.2 Serial Ports 116
3.6.3 Modbus 117
3.6.4 DNP3 126
3.6.5 I/O Settings (IndustrialPro and RAM-6000 Series) 146
3.6.6 I/O Settings (RAM 9000 Series) 148
3.7 Advanced Tab 159
3.7.1 IP Fallback 159
3.7.2 IP Transparency 161
3.7.3 Out-of-Band Management 164
3.7.4 VRRP (Virtual Redundancy Protocol) 166
3.7.5 Expert Mode 167
3.7.6 Gwlnx 170
3.7.7 Classic View 180

Chapter 4 Red Lion Support 181

Chapter 5 Compliance Statements & User Information 182

Chapter 6 Licensing & Warranty 183

Chapter 7 Appendices 184

Appendix A: RED-LION-RAM.MIB Contents 184

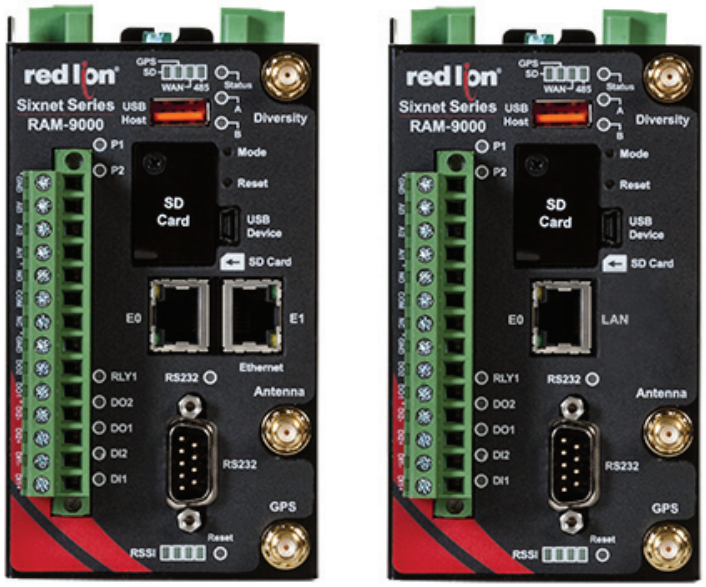
This manual applies to the following products:

SN/RAM-6800	SN/RAM-6801	SN/RAM-6801EB	SN/RAM-6821	RAM 9701
SN/RAM-6600	SN/RAM-6601	SN/RAM-6601EB	SN/RAM-6621	RAM 9711
SN/RAM-6700	SN/RAM-6701	SN/RAM-6701EB	SN/RAM-6721	

Chapter 1 Accessing the Web User Interface

1.1 Connect PC to Red Lion Router

Connect a CAT-5 or CAT-6 Ethernet cable between the local PC and the Red Lion router's Ethernet Port(s).



Note: If the Ethernet port's green LED is lit, this indicates that the connection is running at 100Mb speed. If the Ethernet port's green LED is not lit, this indicates that the connection is running at 10Mb speed. The yellow LED indicates the "link" status of the connection.

Yellow steady= Link established. Yellow flashing = Data packets are being transferred.

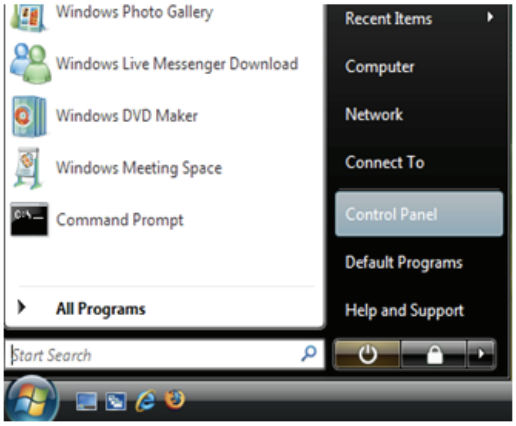
1.2 Setup PC IP Address

1.2.1 Open the Control Panel

- Click on Start and browse the “Control Panel” menu item. The Control Panel should look similar to the following:

XP

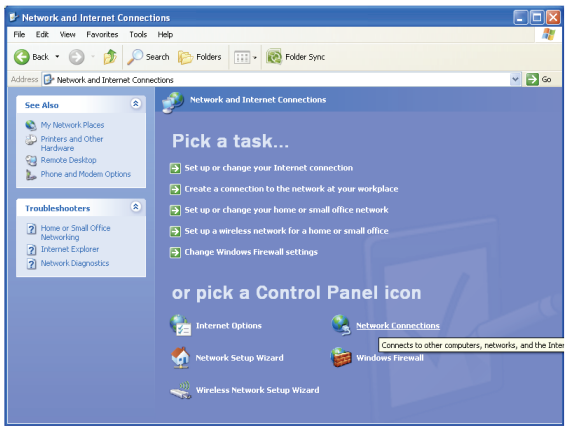
Vista/Windows 7



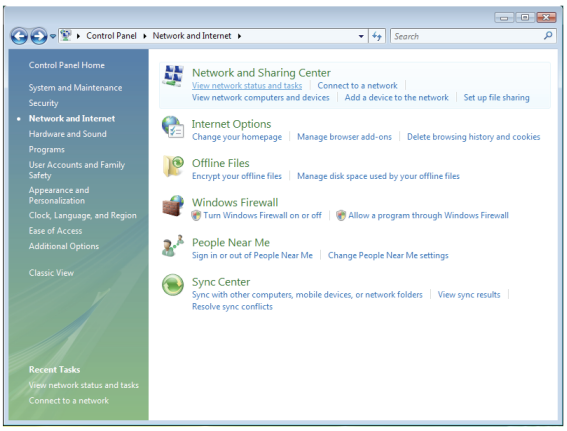
1.2.2 Access Network and Settings

- Click on the link to access network and Internet settings
  - XP - “Network and Internet Connections”
  - Vista/Windows 7 “Network and Internet”
- The displays should be similar to the following:

XP


Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

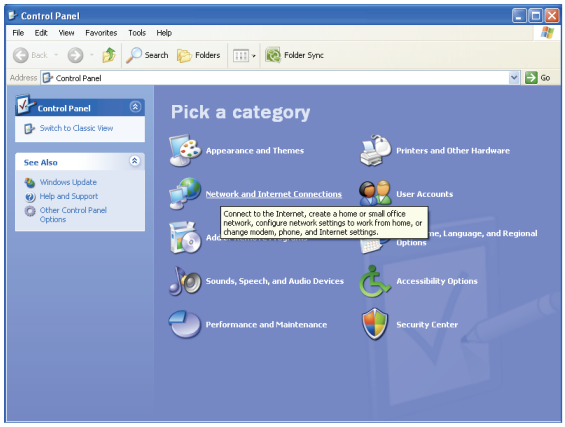
VISTA/WINDOWS 7



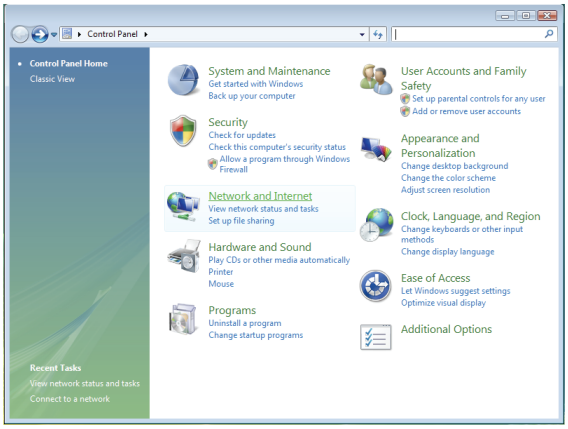
1.2.3 Access Network Connection Settings

- Click on the link to access network connection settings.
  - XP - “Network Connections”
  - Vista/Windows 7 - “Network and Sharing Center”
- The display should look similar to the following:

XP


Control Panel
File Edit View Favorites Tools Help
Search Folders Folder Sync
Address Control Panel
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Other Control Panel Options
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Connect to the Internet, create a home or small office network, configure network settings to work from home, or change modem, phone, and Internet settings.
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance
Security Center

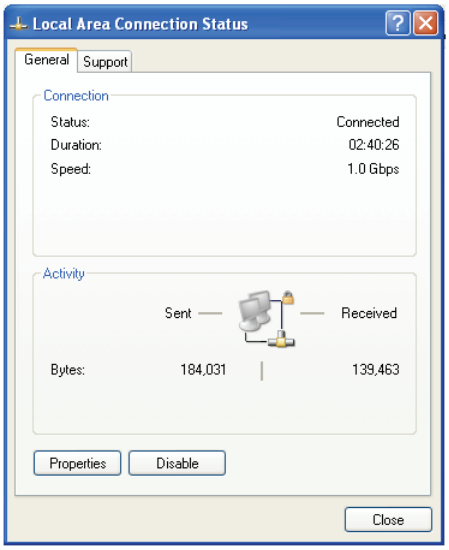
VISTA/WINDOWS 7



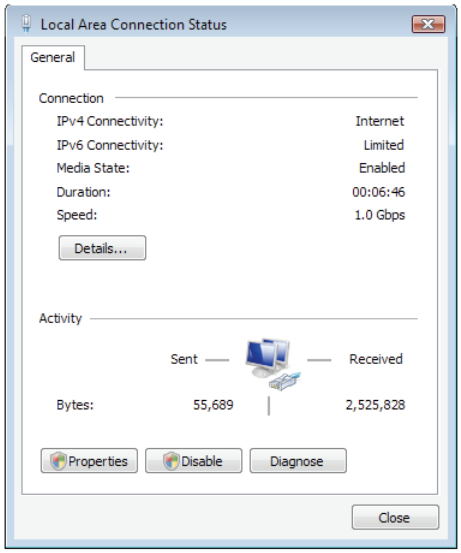
1.2.4 Access Local Area Connection

- Click on the link to access the local area connection.
  - XP - “Local Area Connection” icon
  - Vista/Windows 7 - “View Status” next to Local Area Connection
- The display should look similar to the following:

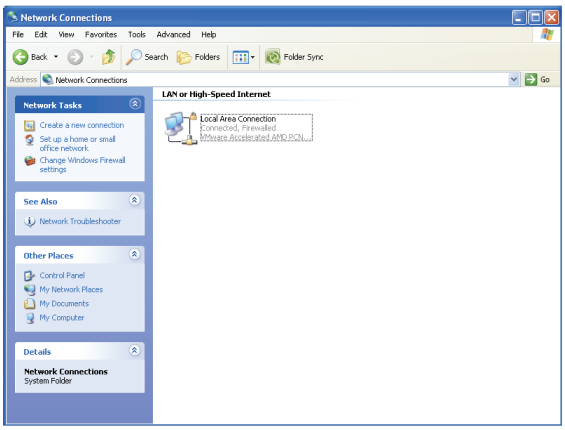
XP



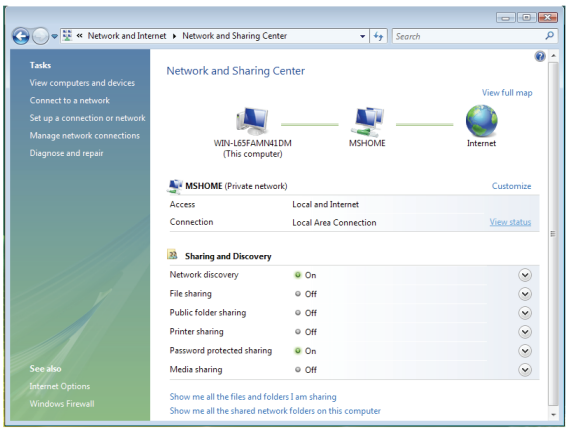
Vista/Windows 7



XP



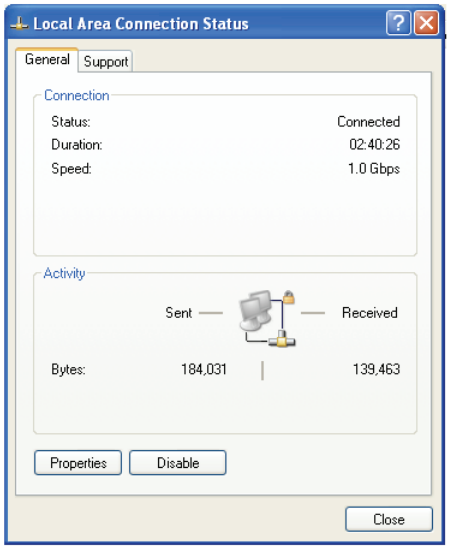
Vista/Windows 7



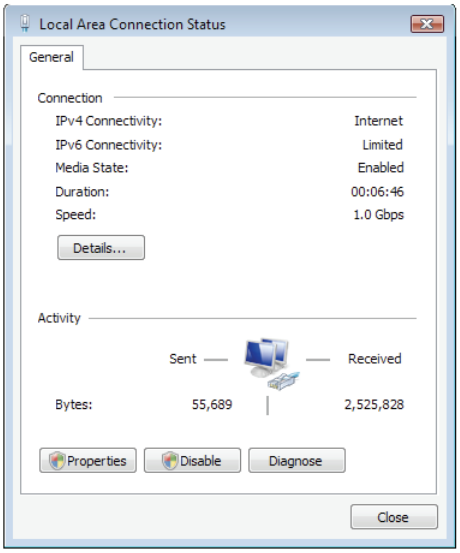
1.2.5 Open Properties

- Click on “Properties” button (Vista/Windows 7 will display a popup window asking to confirm the operation).
- Click on the “Continue” button. The display should look similar to the following:

XP



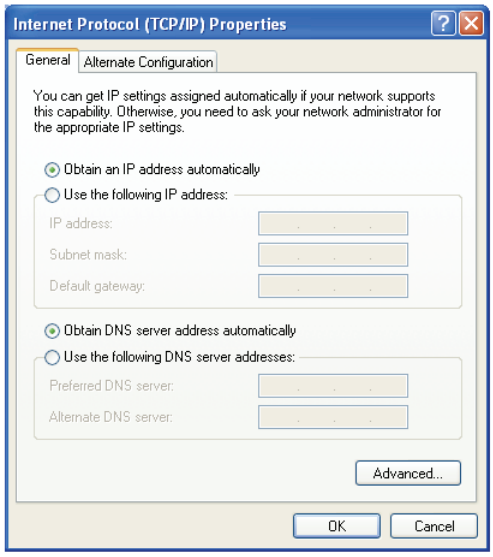
Vista/Windows 7



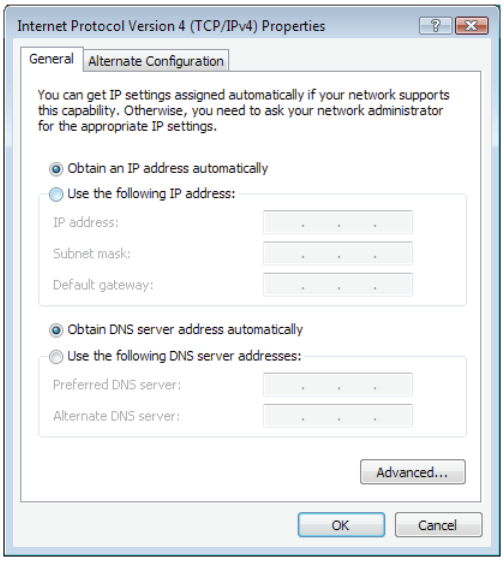
1.2.6 Access Internet Protocol Properties

- Click on the Internet Protocol to highlight.
  - XP - “Internet Protocol (TCP/IP)”
  - Vista/Windows7 - “Internet Protocol Version 4 (TCP/IPv4)”
- Click on the “Properties” button. The display should look similar to the following:

XP

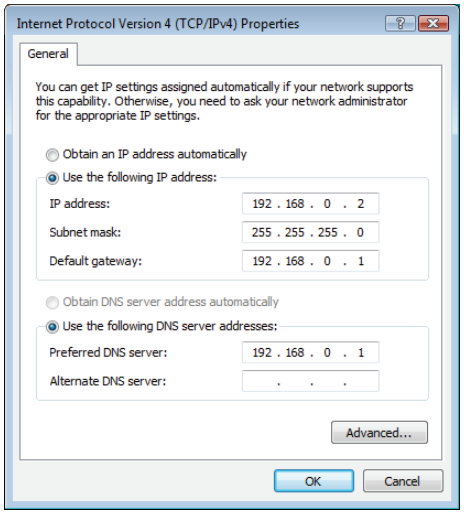

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Vista/Windows 7


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

METHOD 1: PC to: WAN /ETH0, Ethernet on SN/RAM-6000, RAM 9000

- Select “Use the following IP address” and fill in the blank fields with the information below:

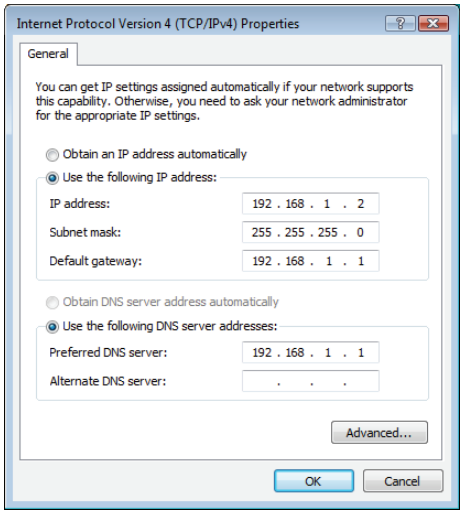

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:
Advanced...
OK
Cancel

- IP address:192.168.0.2
- Subnet mask:255.255.255.0
- Default gateway:192.168.0.1
- Preferred DNS:192.168.0.1

- Click “OK”.
- The previous screen will appear.
- Click “OK”.

METHOD 2: PC to LAN: ETH1, RAM 9000 Series only

- Select “Use the following IP address” and fill in the blank fields with the information below:

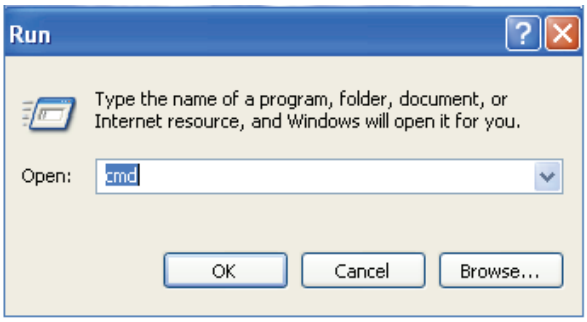

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

- IP address:192.168.1.2
- Subnet mask:255.255.255.0
- Default gateway:192.168.1.1
- Preferred DNS:192.168.1.1

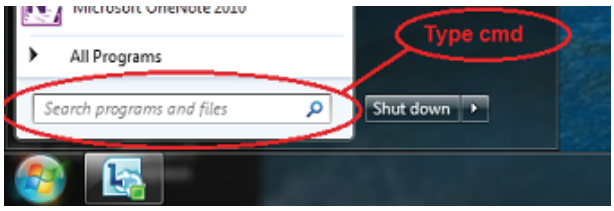
- Click “OK”.
- The previous screen will appear.
- Click “OK”.

Verify that you are connected to the router.

- Open a Command Prompt window on your laptop.
  - XP →Start →Run, type in **cmd** and press the **ENTER** key.



  - Vista/Windows 7 →Start →Search window just above the Start icon, type in cmd, wait for Vista/Windows 7 to locate the program, click on the cmd program if finds.

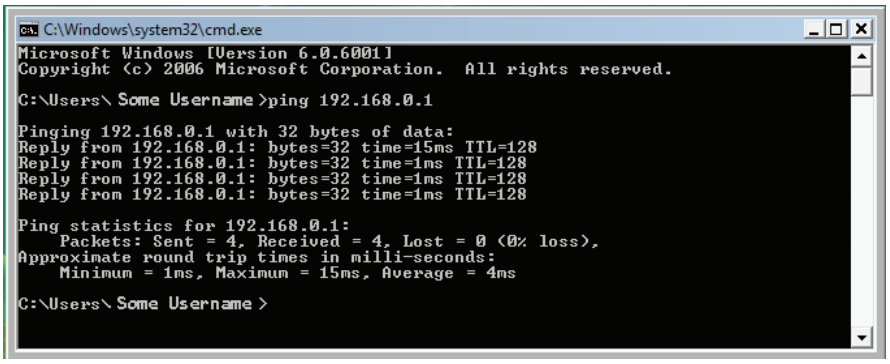


Verify connectivity to the router by running a “ping” to the IP Address of the Ethernet port you are connected to.

METHOD 1: PC to WAN /ETH0, Ethernet on SN-6000, RAM 9000

Type in **ping 192.168.0.1** and then press the **ENTER** key

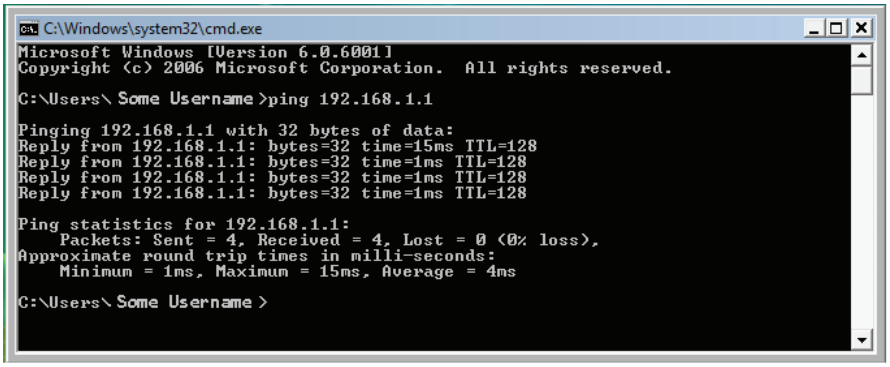
The display should look similar to the following:


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\ Some Username >ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=15ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 15ms, Average = 4ms
C:\Users\ Some Username >

METHOD 2: PC to ETH1: LAN on RAM 9000 only

Type in **ping 192.168.1.1** and the press the **ENTER** key

The display should look similar to the following:


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\ Some Username >ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=15ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 15ms, Average = 4ms
C:\Users\ Some Username >

This shows the connection is up and functioning.

1.3 Access Red Lion Web Server

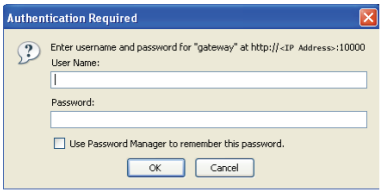
- Open a web browser and enter the following in the address bar:

  METHOD 1 (WAN/ETH0): http://192.168.0.1:10000/

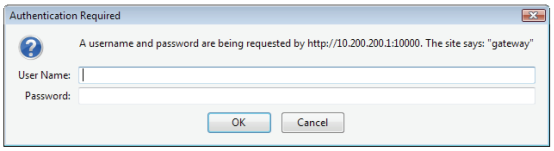
  METHOD 2 (LAN/ETH1): http://192.168.1.1:10000/

- You will receive a login pop-up screen.

XP



Vista/Windows 7

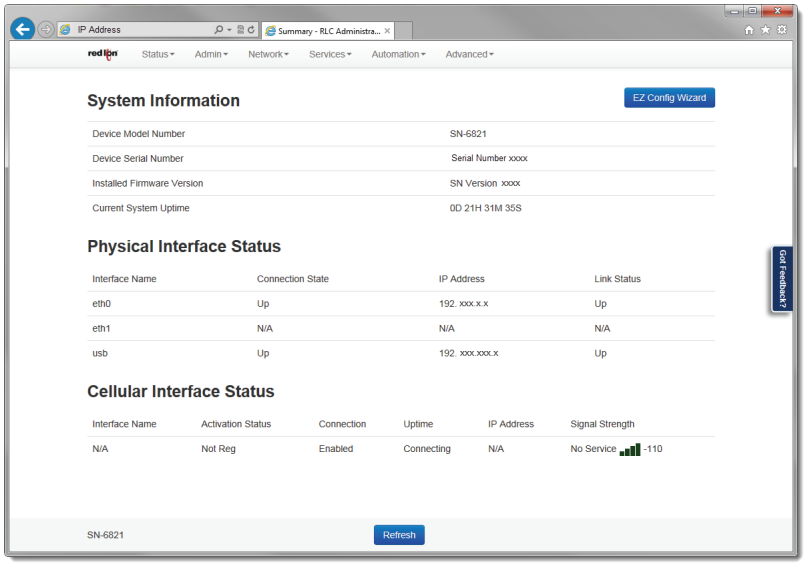


1.3.1 Red Lion Router Login Instructions

- For the User Name, enter: **admin** (all lowercase)
- For Password, enter the **last six digits of the serial number**, located on the product label (all lowercase)

Upon successfully logging in, the following screen will appear:

Note: The following information can be used for all series of router, even if screen shots indicate other models. Some models may have reduced options.



At this point, you are connected to the Red Lion router and can configure it to meet your needs.

If the ppp0 or wwan0 interface do not show an IP address, this could indicate that the internal SIM/Module has not been properly activated. Low or invalid signal strength may also contribute to the issue. Please contact your service provider to ensure proper activation. You may need to enter provisioning information in the Networking→Cellular→Provisioning screen. Consult Section 2.1 for more information.

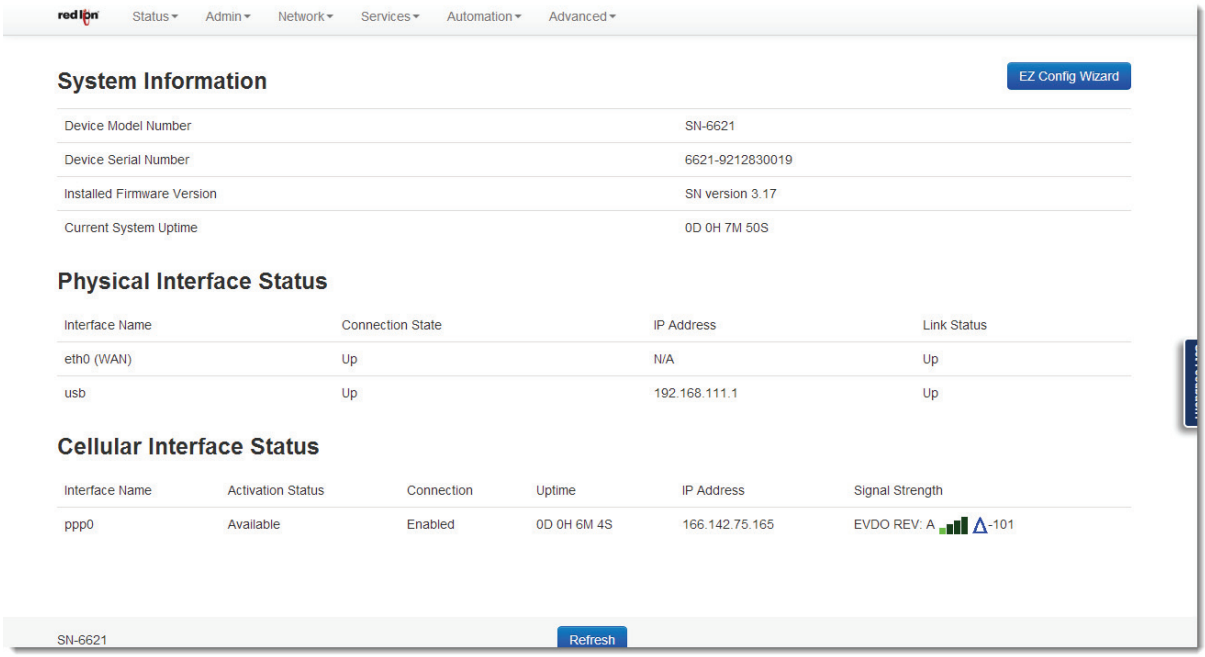
1.3.2 SSH, Telnet, Serial RS-232 Connections to Red Lion Routers

For alternative connections to the Red Lion router, please contact Red Lion Technical Support for additional documentation.

Chapter 2 Cellular Connections

2.1 Cellular Configuration

Cellular connectivity can be obtained through the use of an internal (embedded) RF Module.



Your Red Lion router has an embedded cellular radio that is already detected and configured for the intended carrier. If you are using a carrier that supports the use of an APN, you may have to set your specific APN manually, as covered in the next section. For GSM and LTE service, carriers may provide custom APNs for static IP addresses of VPNs scenarios depending on the type of account.

CDMA carriers such as Verizon and Sprint 3G do not rely on a SIM card and are activated over the air. See the Cellular Provisioning section of the manual for more details on CDMA OTA activations.

Embedded modules for CDMA (Sprint / Verizon) should activate automatically over the air once they are powered on and connected to an antenna. This of course is after you contact your carrier and have an account enabled and connected to the embedded module by providing the ESN / MEID number from the module to your carrier. This is how the carrier will tie your account to the internal cellular radio. For some CDMA based 1xRTT internal modules and Sprint Data-Link connections, additional configuration must be set in the Provisioning screen, detailed later.

Navigate through the Web UI menu to Networking → Cellular Connection → Configuration screen shown in section 2.1.1. GSM based carriers, such as AT&T, Bell Mobility and Telus will require a SIM card be inserted into the unit and an APN code to be entered to confirm you are the verified user of that SIM. Be sure to only insert and remove the SIM card while the unit is powered off.

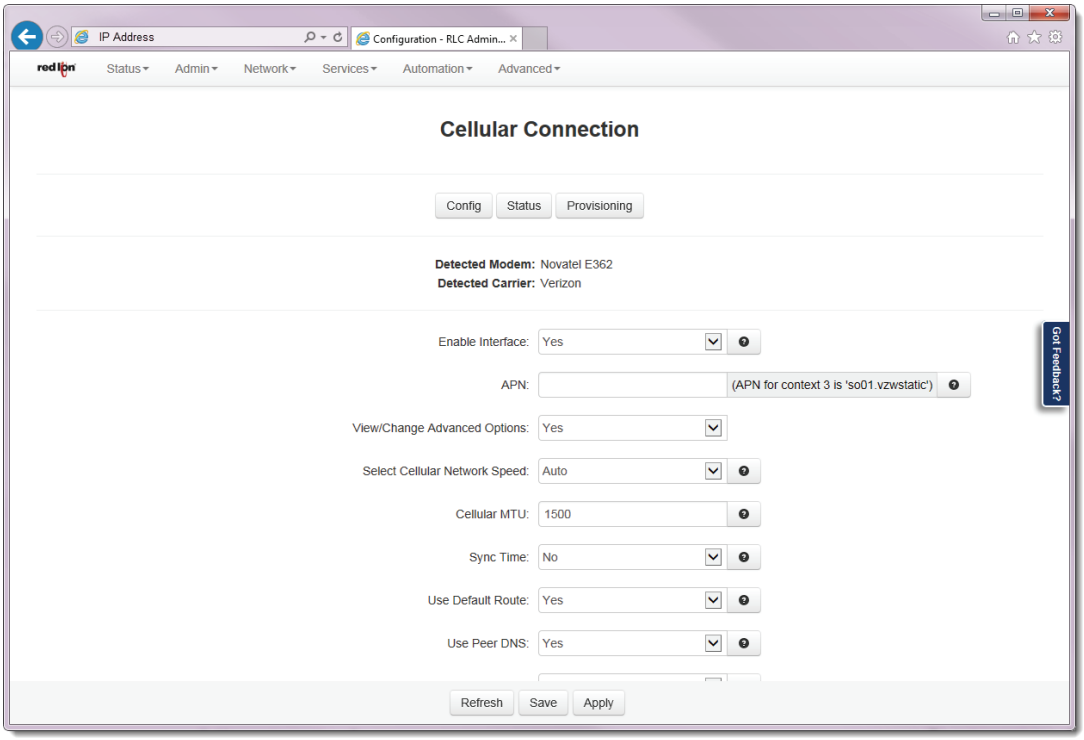
You can verify your cellular connectivity by viewing the Status Summary page of the web UI screen and observe if the Cellular Interface status shows an IP Address. On the Home screen you should see: Interface, Activation, Connection, IP

Address and Signal Strength. If you do not see an IP Address get populated for the PPP interface you may have an issue with your settings or your account has not been correctly activated.

Activation Status column: See table below for a description of the different statuses found in the “Activation Status” column.

CDMA	HSPA/LTE
Running - Connection/Activation is running	Not Reg - Modem not registered
Waiting - Connection/Activation tried and failed. Will retry in 20 mins.	Reg Home - Registered on Home Network
Succeeded - Connection/Activation successful	Searching - Searching for connection
Unavailable - connection/Activation not supported	Reg Denied - No SIM or SIM no longer activated
Failed - Connection/Activation Failed	Unkn Stat - Unknown status
Available - Activation not running/Module has not tried to connect/Module already activated	Reg Roam - Registered on roaming network

2.1.1 Cellular Interface Configuration



- Select Yes to enable the interface so it becomes active after the new settings are applied and upon subsequent system start-up. Select No to disable the cellular connection feature. More information on setting up the unit’s cellular connection can be found in section 3.4.1.

2.1.2 Set the User Name, Password and APN

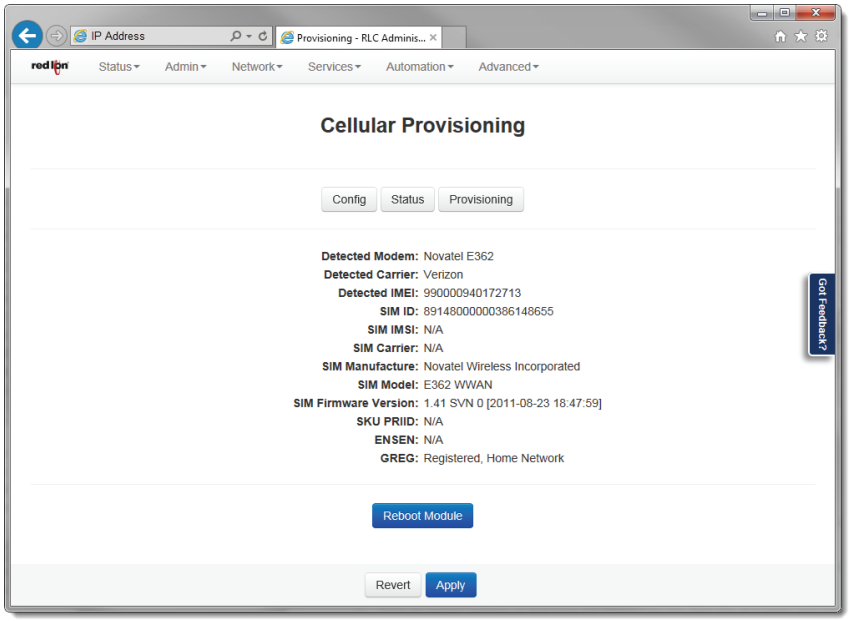
If you are using a GPRS, Edge or HSDPA based card, enter the User Name, Password and APN that was provided by your cellular carrier. This information should have been packaged with your SIM chip. If you do not have this information, please contact your carrier’s account representative or the carrier’s support department before proceeding.

Click the “Apply” button to save and activate the configuration.

Note: The User Name, Password and APN can be case sensitive. Be certain that you use the exact information as provided by your carrier.

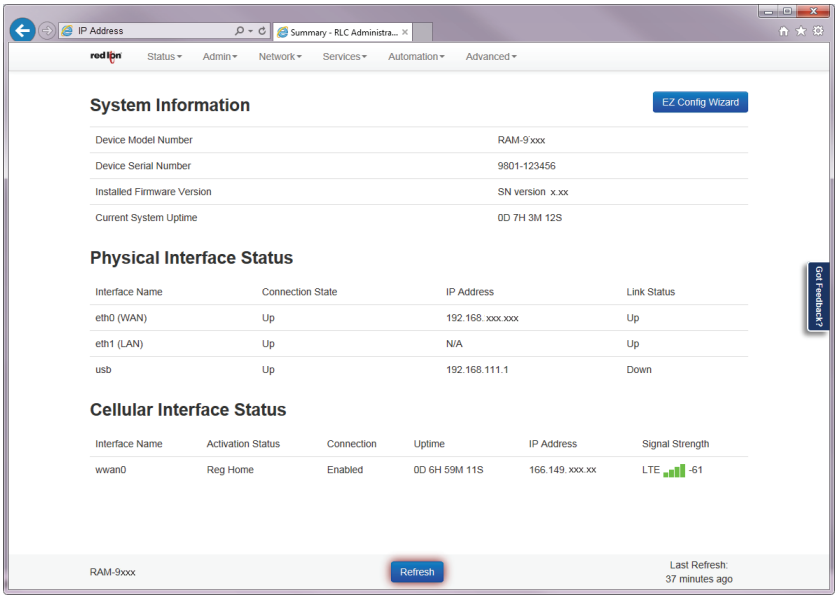
2.1.3 Provisioning

For Sprint/CDMA installations for Sprint Data link support, additional information may be required. Navigate to Network -> Cellular Connection -> Provisioning.



2.1.4 Verify Cellular Connectivity

Browse to the Status screen, by selecting Summary -> Status. The following dialog window will appear:


IP Address
Summary - RLC Administra...
Status
Admin
Network
Services
Automation
Advanced
System Information
EZ Config Wizard
Device Model Number RAM-9 xxx
Device Serial Number 9801-123456
Installed Firmware Version SN version x.xx
Current System Uptime 0D 7H 3M 12S
Physical Interface Status
Interface Name | Connection State | IP Address | Link Status
eth0 (WAN) | Up | 192.168. xxx.xxx | Up
eth1 (LAN) | Up | N/A | Up
usb | Up | 192.168.111.1 | Down
Cellular Interface Status
Interface Name | Activation Status | Connection | Uptime | IP Address | Signal Strength
wwan0 | Reg Home | Enabled | 0D 6H 59M 11S | 166.149. xxx.xx | LTE -61
RAM-9xxx
Refresh
Last Refresh:
37 minutes ago
Got Feedback?

As shown, the router is receiving good signal from the cellular network, it is connected and has been issued an IP address.

At this point, if you previously verified that the SIM/Module is activated and have been accessing the web UI to configure your Red Lion interface via it's browser, you should be able to access the Internet.

- Open a browser on the PC/Laptop, and attempt to browse the Internet.

NOTE: Depending on the provisioning of your module/SIM, particularly in corporate applications in which the unit is providing cellular backup connectivity to wired circuits, your module/SIM may be restricted from Internet access. If this is the case, you may want to test to ensure that you are able to access your corporate network. If you have any questions about your configuration, please check with your network adminstrator.

If you were able to successfully access the Internet, or your corporate network, your Red Lion unit is up and running. You have successfully completed the Quick Start and you may skip the troubleshooting section.

2.1.5 Cellular Connectivity Troubleshooting

NOTE: If you were unable to access the Internet, or your corporate network, the section that follows will help you to determine the cause of your difficulties.

If you are reading this section, you have followed all previous instructions and your Red Lion router is not communicating, this section will provide additional information to isolate the cause of difficulties.

2.1.5.1 Cellular Reception

Before we get into specifics regarding how to identify and address specific problems that can be encountered, it is important that we spend a moment talking about cellular signal reception, and appropriate expectations.

All of the major cellular carriers expend significant sums insuring that we have excellent signal coverage within their coverage areas. However, they have no control over the environments in which we attempt to place or use our cellular devices.

The principles behind cellular data reception are similar to cellular phone reception. Therefore, our environment has the potential to significantly impact our ability to receive a good quality cellular signal.

You should be aware that it is possible to stand in the parking lot of a building and have perfect reception, but walk just 10 feet inside a concrete and steel building and have absolutely no reception at all.

The important thing to understand is that in many, many instances it is not the cellular network that causes reception problems, but the environment in which we place our cellular devices.

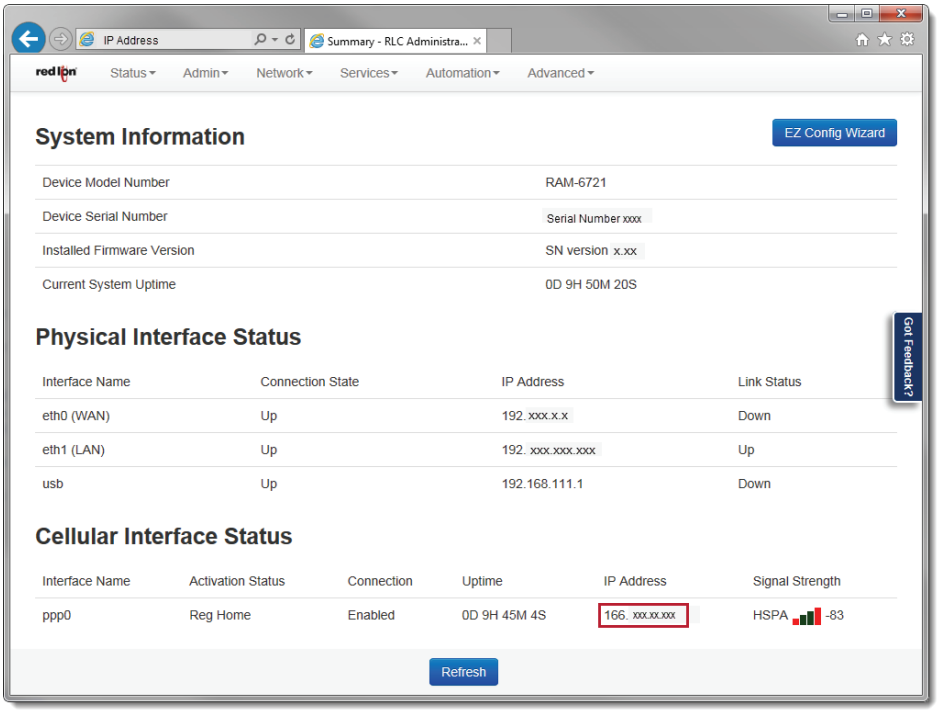
Important Note about Cellular Antennas

For this reason, Red Lion strongly recommends the use of external antennas when implementing cellular data. It is often the key to a successful implementation. Consult your Red Lion representative if you have questions about the appropriate use of external antennas.

2.1.5.2 Verifying IP Connectivity

First, check to make sure that your device is connecting to the cellular network and obtaining an IP address.

Navigate to the Web UI Status screen shown below:

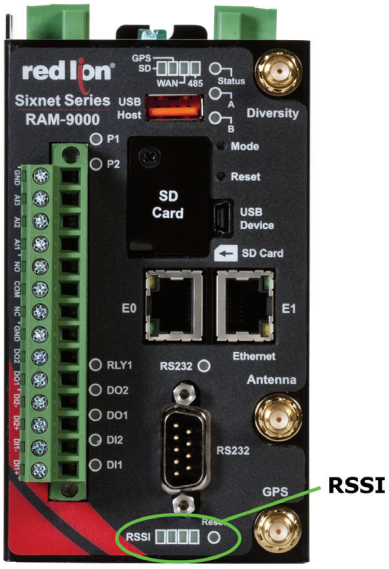


If your screen looks similar to the one shown above, you are having signal reception difficulties. You can further verify this condition by examining the LED signal meter.

SN6000 units: Observe the signal LED as shown below.

Signal	OFF	No signal available or signal strength is below -100 dBm
	ON	Excellent signal strength = greater than -69 dBm
	FLASH	Fast: Every 300ms = -79 to -70 dBm
		Medium: Every 600ms = -89 to -80 dBm
		Slow: Every 1200ms = -99 to -90 dBm

RAM 9000 units: Observe the RSSI LED as shown below.

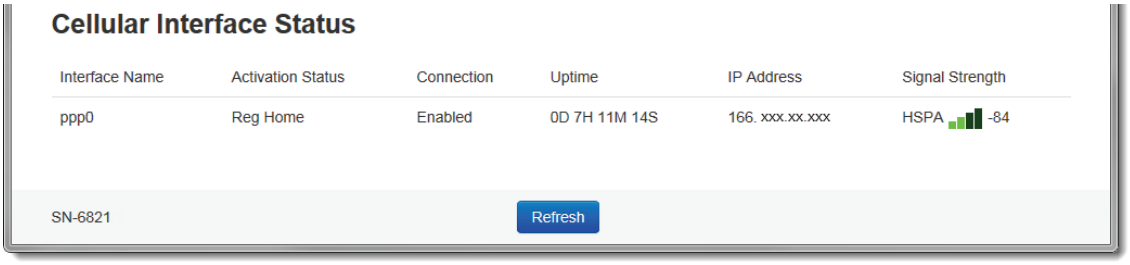


RSSI		Low Signal / No service
		≥ - 109 dBm (Low but valid signal)
		≥ - 99 dBm (Lower but valid signal)
		≥ - 89 dBm (Avg signal)
		≥ - 80 dBm (Excellent signal)

2.1.5.3 Minimal Reception

On occasion, you can find yourself in a situation where you have just enough signal to be able to communicate with the cellular tower and obtain an IP address, but not enough reception to be able to sustain a viable connection.

If your cellular card is using dynamically assigned IP addresses, you can determine if you are in a situation like this by watching the “Cellular Interface” field from the Home screen (Summary -> Status) as shown below:

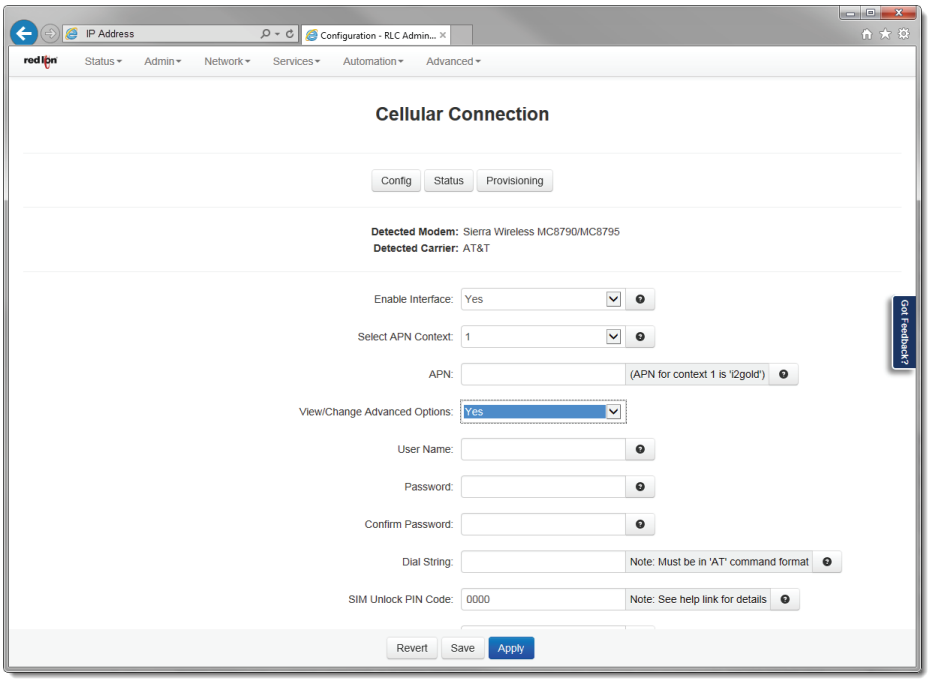


If you refresh this screen every few minutes and notice that the IP address is changing frequently, it is possible that the router is connecting to the network and obtaining an IP address and then the connection to the cellular network is being dropped. When the connection is re-established, the device is then issued a different IP address.

2.1.5.4 Authentication Issues

If you are using a GPRS/EDGE/HSDPA card, and have at least three LEDs of signal on the front panel signal meter, your radio connection to the network may be just fine. The problem may lie in logging onto the cellular network.

Navigate to the Cellular Connection dialog window (Network -> Cellular Connection -> Configuration):



Verify your user name, password, and APN information. All three of these items can be case-sensitive and must be entered exactly in order to properly log in to the cellular network.

- Click on the “Save” button for changes to be saved without activating the interface, the “Apply” button will save your settings and apply them immediately. To revert to the previous settings, click on the “Revert” button.

2.1.5.5 Red Lion Technical Support

If you have followed all of the instructions up to this point, have satisfied yourself that you are not having an authentication problem, are convinced that you have sufficient reception, and your router is still not communicating, then please call Red Lion Technical Support at 1-877-432-9908. Live support is available from 8:00 a.m. - 5:30 p.m. EST. If you call after hours, please leave your contact information and a detailed description of your problem and we will respond to you the following business day. We will be happy to assist you in getting your router operational.

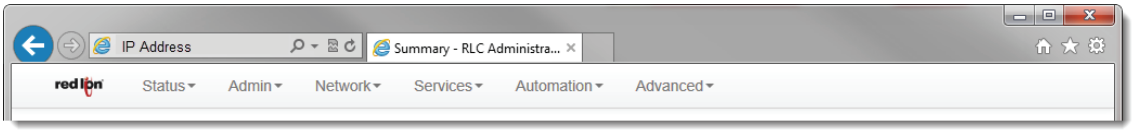
When submitting a support question, it is most helpful to have a GatherStats from the unit in question. Please obtain one from the Status -> GatherStats screen. Choose the Download Option, and save the resulting file to your PC. You may attach it to an email to support@redlion.net, describing your issue.

Chapter 3 Web User Interface

3.1 Web User Interface Introduction

3.1.1 Organization

The Red Lion Web UI is comprised of six major sections. *(Click on a link to get an in-depth description of each topic)*

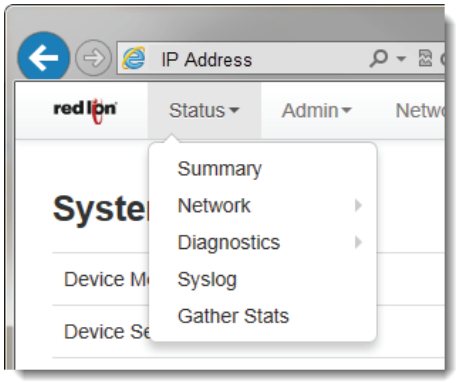


- Status: The Status tab presents information on the router. This tab is organized into five (5) sections: Summary, Network, Diagnostics, Syslog and Gather Stats.
- Admin: The Admin Tab is used to configure how the Red Lion router is accessed, update the firmware, reset the system defaults, set the system time and reboot the router remotely. This tab is organized into six (7) sections: Access Settings, System Time, Certificate Manager, Firmware Update, Configuration Manager, Package Installation and Factory Defaults/Reboot.
- Network: The Network Tab is used to configure settings that connect the router to external interfaces. The Network tab is organized into seven (7) major categories: Cellular Connections, Interfaces, Firewall, Tunneling, DNS Settings, Static Routes and TCP Global Settings.
- Services: The Services tab is used to configure the various features of the Red Lion router. These services include DHCP Server, DHCP Relay, Dynamic DNS, SNProxy Settings, SixView Manager, GPS Settings, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive and Serial IP.
- Automation: The Automation menu contains all aspects of managing your Modbus and DNP3 based I/O. The Automation tab is organized into five (5) categories: Local Station, Serial Ports, Modbus, DNP3 and I/O Settings.
- Advanced: The Advanced Tab is used to configure the advanced features of the Red Lion router, which include IP Fallback, IP Transparency, Out-of-Band Management, VRRP, Expert Mode, GWLNX, Classic View and About.

All tabs are described further in the manual as well as functionality of each dialog window.

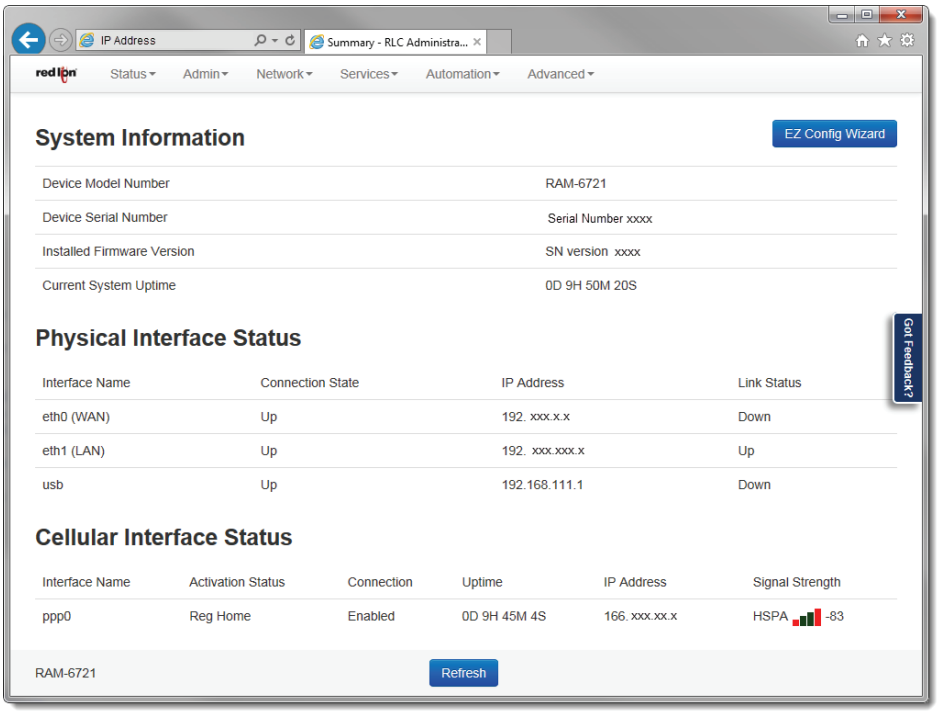
3.2 Status Tab

The Status Tab allows you to review the state of the router functions, such as network connections, interfaces, system processes, services running, and system information. It also allows review of the syslog, update history, and under diagnostic tools, permits testing connectivity through the use of ‘ping’ and ‘traceroute’.



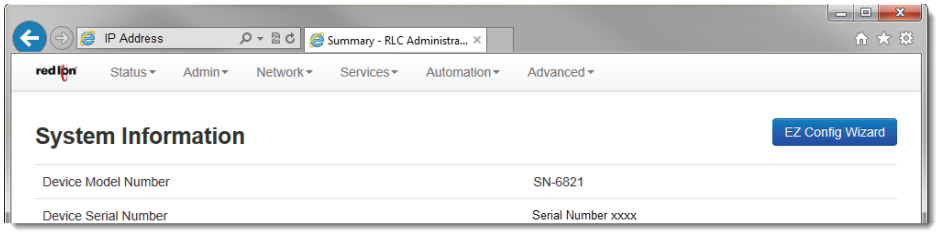
3.2.1 Summary

This option will return the user to the System Summary (home) page. On this page, the system information and physical interface status are easily viewed.

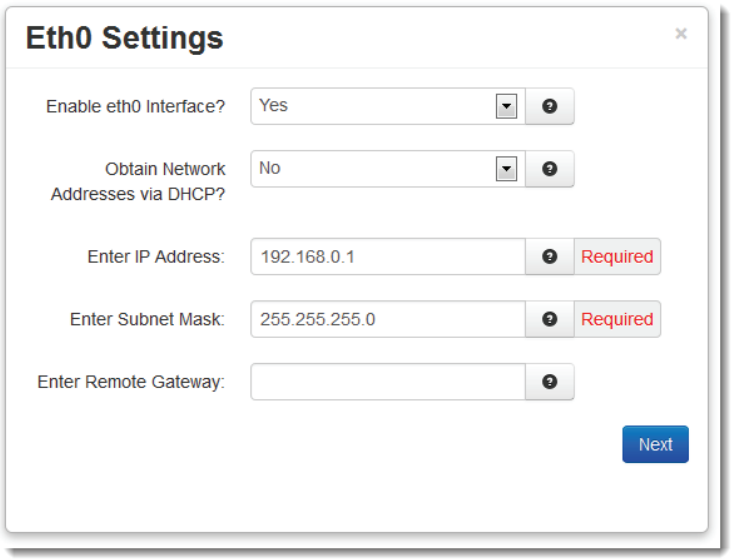


3.2.1.1 EZ Config Wizard

The EZ Config Wizard is used to setup your Ethernet IP without having to navigate through multiple dialog windows. The EZ Config Wizard is situated on the Summary page and accessed by clicking on the blue EZ Config Wizard button.



- Click on the EZ Config Wizard button. The Eth0 Settings dialog window will open:



Enable eth0 Interface: Select *Yes* to enable the interface or No to disable it. If you select *No*, the fields below the "Enable eth0 Interface" will disappear.

Obtain Network Addresses via DHCP: Select *Yes* to allow the interface to obtain address information via a DHCP server. The device will obtain its IP address, netmask and remote gateway as the default route. It can also, optionally, obtain DNS server address via DHCP.

Select *No* to prevent the interface from obtaining address information via a DHCP servers.

You will be required to enter the IP address, netmask and remote gateway addresses. DNS information can be provided by navigating to the Network>DNS Settings menu.

Enter IP Address (Required): Enter the desired interface IP address. This field is only available when the "Obtain Network Addresses via DHCP" is set to *No*.

The IP address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the broadcast address.

Recommended Setting: This address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the Enter Subnet Mask field and must not conflict with any other device on the target network.

Enter Subnet Mask (Required): Enter the desired Netmask for the interface. This field is only available when "Obtain Network Addresses via DHCP" has been set to *No*.

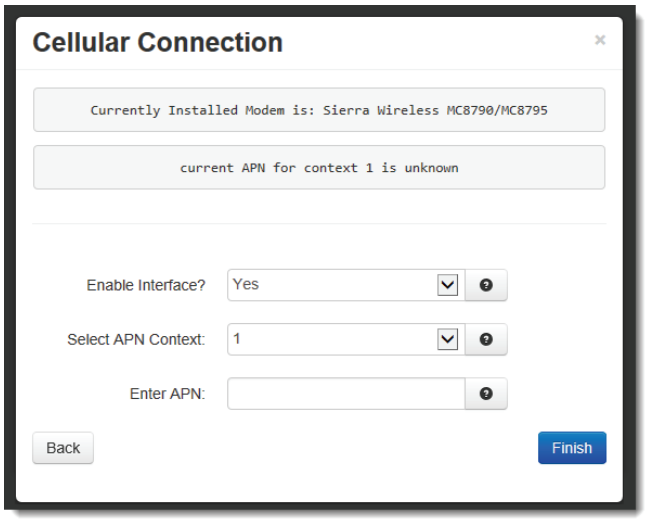
Recommended Setting: Your network administrator should be able to provide an appropriate value. This value determines the valid range of IP addresses allowed in the "Enter IP Address" field.

Enter Remote Gateway: Enter the IP Address for the gateway device. This field is required if "Use Remote Gateway as Default Route" is set to *Yes*.

A gateway is a device (typically a router) used to gain access to another network. For example, if a device is attached to a LAN whose network address is 192.168.1.0 with a netmask of 255.255.255.0, then it can communicate directly with any other device on that network with a range of addresses of 192.168.1.1 through 192.168.1.254 (with 192.168.1.255 reserved for broadcast). An address outside of that range is on a different network which would need to be accessed indirectly through a router. That router would be the gateway to the network on which the remote target device resides. In order to communicate with it, it would mean sending and receiving via the gateway device. This also requires either defining a static route (defined through the Network>Static Routes menu) via that gateway or making it the default route by setting "Use Remote Gateway as Default Route" to *Yes*.

Recommended Setting: Your network administrator should be able to provide an appropriate value. The address must be one within the valid range for the network.

- Once the desired settings have been entered in the Eth0 Settings dialog window, click on the Next button and the following Cellular Connection dialog window will appear:



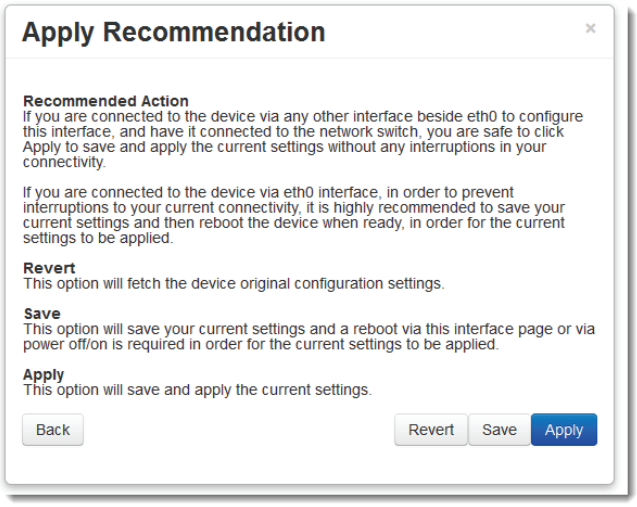
Enable Interface: Select YES to enable the interface to become active after the new settings are applied and upon sub-sequent system start-up.

Select APN Context: Select the desired APN Context from the provided drop-down. This information should have been given to you by your service provider when service was established.

Enter APN: Enter the APN used to access your cellular wireless data service in this field. This information should have been given to you by your service provider when service was established.

Note: Entering an APN value in this field will overwrite any APN stored in the modem for the selected context.

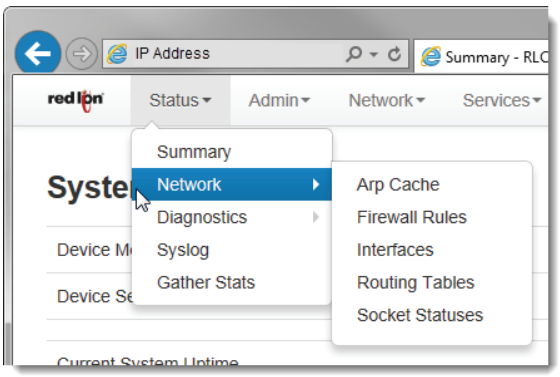
- Once the desired settings have been entered, click on the Finish button and a recommendation dialog window will appear.


Apply Recommendation
Recommended Action
If you are connected to the device via any other interface beside eth0 to configure this interface, and have it connected to the network switch, you are safe to click Apply to save and apply the current settings without any interruptions in your connectivity.
If you are connected to the device via eth0 interface, in order to prevent interruptions to your current connectivity, it is highly recommended to save your current settings and then reboot the device when ready, in order for the current settings to be applied.
Revert
This option will fetch the device original configuration settings.
Save
This option will save your current settings and a reboot via this interface page or via power off/on is required in order for the current settings to be applied.
Apply
This option will save and apply the current settings.
Back
Revert
Save
Apply

- Click on Revert, Save or Apply (*see explanation of each setting in dialog window above*).

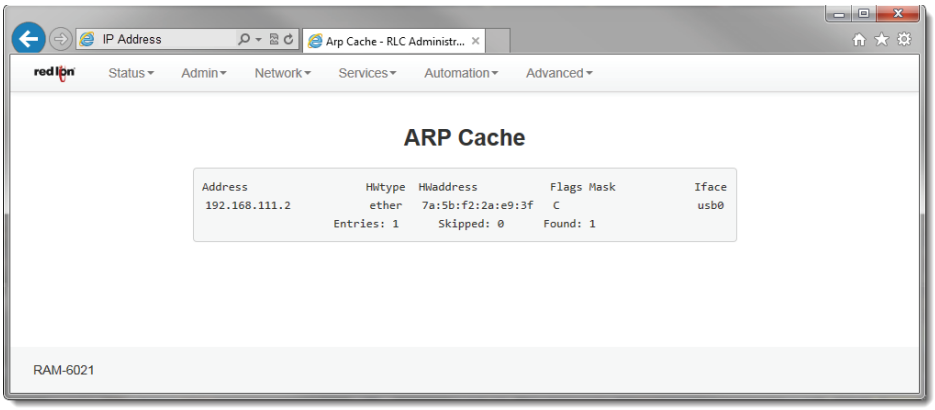
3.2.2 Network

The Network menu contains the following sub-menus: Arp Cache, Firewall Rules, Interfaces, Routing Tables and Socket Statuses.



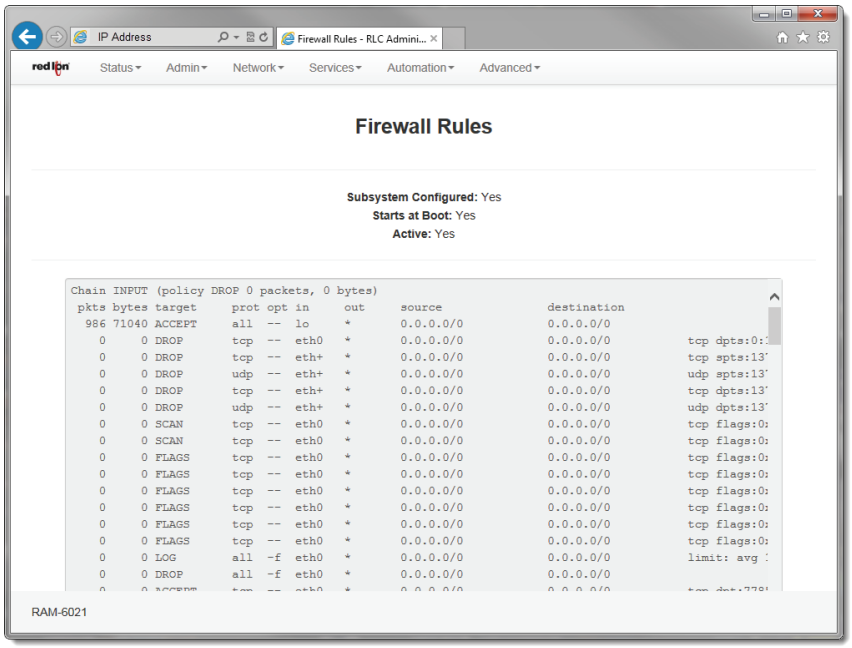
3.2.2.1 ARP Cache

The “ARP Cache” is a table which stores mappings between Data Link Layer (OSI Layer 2) addresses and Network Layer (OSI Layer 3) addresses. This important information shows what connections are established to the router. When you click on the ARP Cache menu item, the following dialog window will appear.



3.2.2.2 Firewall Rules

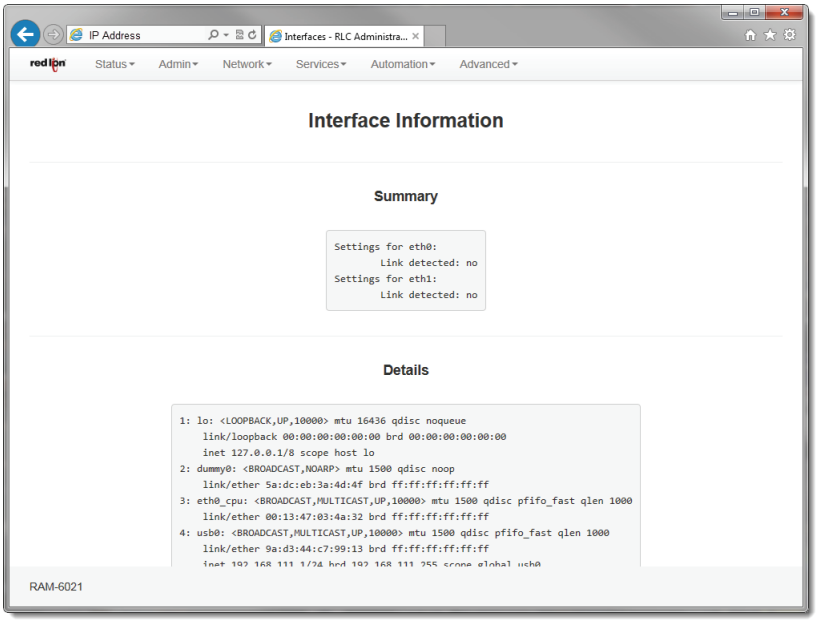
The “Firewall Rules” menu item displays a complete listing of the rules used within the firewall for the Red Lion router. If you are familiar with Linux and IPTables, this will be of great use.



Scroll through the list of rules to review the entire IPTABLES listing. This information is used to track traffic being allowed and traffic being denied access to and through the Red Lion router.

3.2.2.3 Interfaces

The “Interfaces” dialog window is divided into three sections. Summary, Details and Multicast.



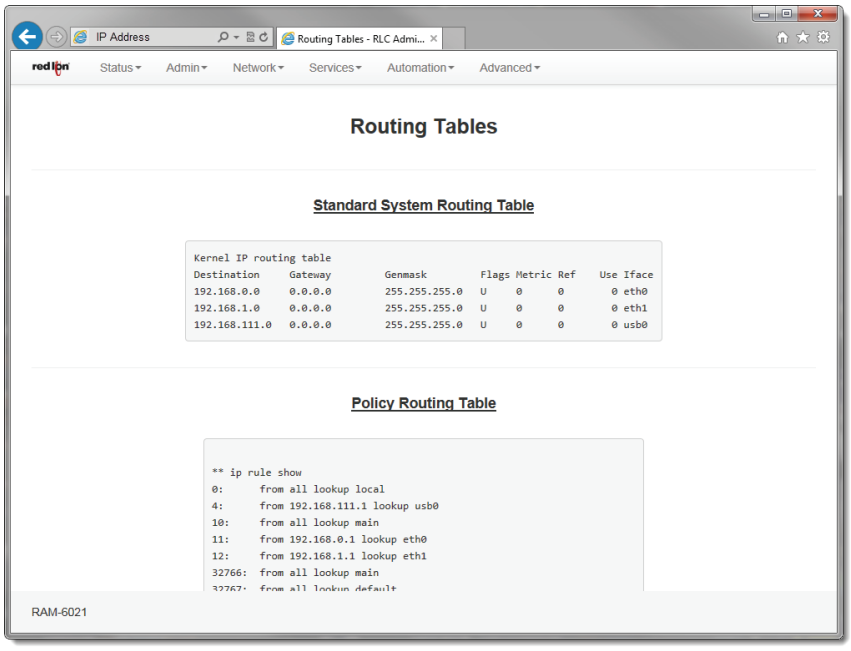
The “Summary” table displays a brief description of the interfaces of the Red Lion router.

The “Details” table displays a system specific description of the interfaces on the Red Lion router.

The “Multicast” table displays the current multicast settings for various interfaces.

3.2.2.4 Routing Tables

The “Routing Tables” dialog window contains both the Standard System Routing Table and the Policy Routing Table.



The “Standard System Routing Table” displays the current routes for the Red Lion router and the static routes that have been configured for the router.

The “Policy Routing Table” displays information on the policy rules, the route tables for each individual interface and the general routes for the Red Lion router.

3.2.2.5 Socket Statuses

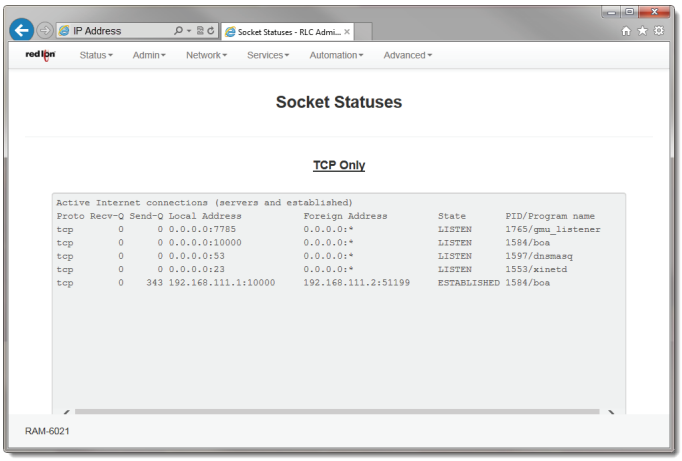
Sockets are end-points to communication over the Internet. Much like PBX phone systems, where the IP address is the phone number and the port is the extension. Every paired (connected) socket has a source IP/port and a destination IP/port.

There are three tables in the Socket Statuses dialog window: “TCP Only”, “Conn Track” and “Socket Statuses All”

The “TCP Only” table displays the sockets that are connection-oriented (Also known as “stream sockets”).

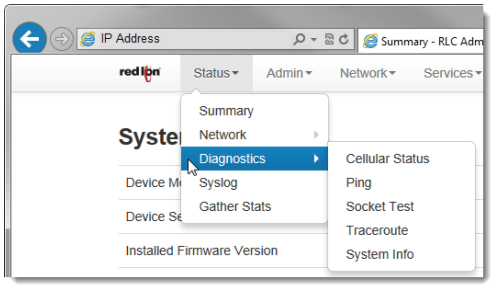
“Conn Track” is a connection tracker that displays more thorough information about the current socket connections. Connection tracking allows the kernel to keep track of all logical network connections or sessions, and thereby relate all of the packets which may make up that connection. NAT relies on this information to translate all related packets in the same way, and IPTABLES can use this information to act as a stateful firewall.

The “Socket Statuses All” table displays the sockets that are considered connection-oriented and connectionless (also known as “datagram sockets”).



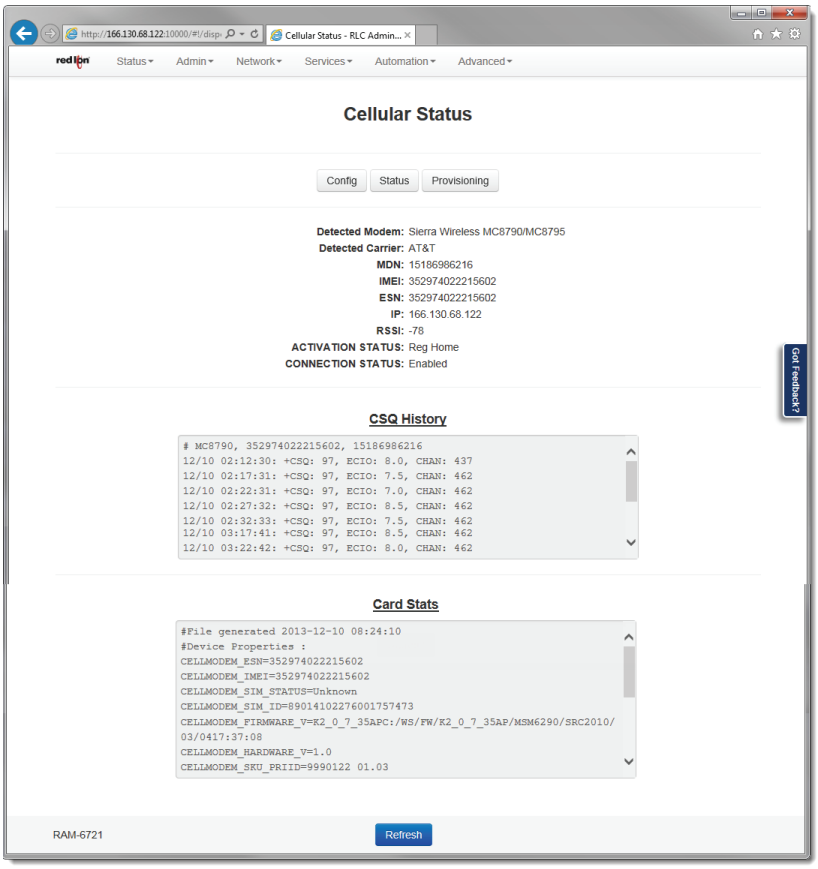
3.2.3 Diagnostics

The Diagnostics menu is sub-sectioned into Cellular Status, Ping, Socket Test, Traceroute and System Info submenus. These are useful in troubleshooting connectivity of the Red Lion router to the Internet or the Network the router is connected to.



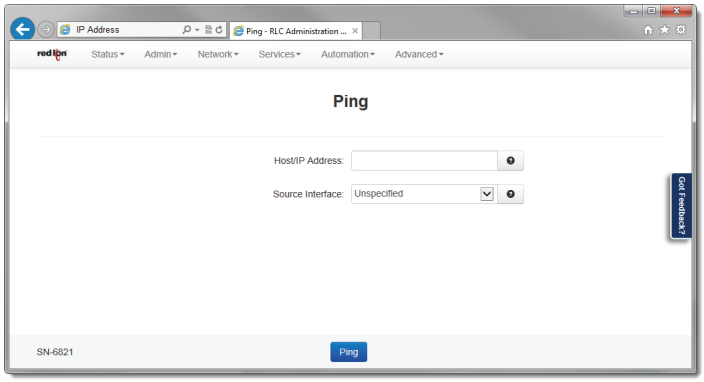
3.2.3.1 Cellular Status

The Status menu item will bring up a dialog window which displays the status of the cellular connection. From here, you can get information such as the type of modem, carrier, MDN, IMEI, ESN, IP RSSI, Activation Status, Connection Status, CSQ Status and Card Stats.



3.2.3.2 Ping

The Ping menu item allows you to input an address either as an IP Address or a URL for testing the destination availability.



Host/IP Address field: Type in the IP Address or URL you wish to Ping. It is recommended you start with a locally accessible IP address to confirm communication to an interface's local subnet. Then proceed to addresses on distant

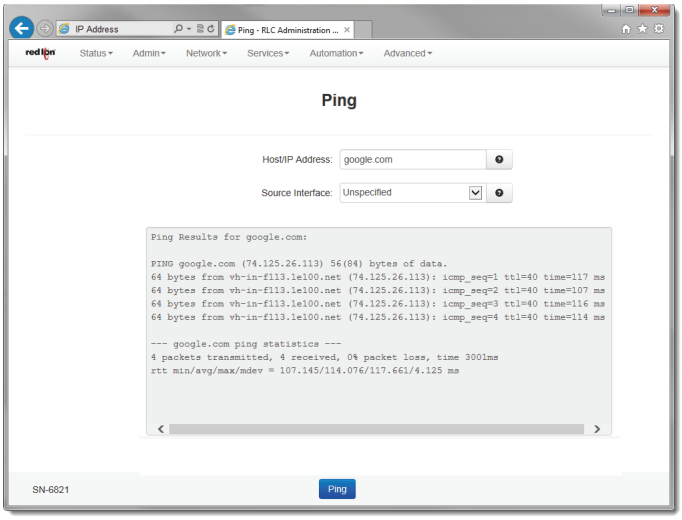
networks. Your local default gateway is a good test, and this IP can be found in the your routing table. Also, a commonly available internet server available to test against is 4.2.2.2

Source Interface: The Source Interface offers the option of using different interfaces to send the Ping through. This is useful if you have a VPN Tunnel in place. Testing the connection through the VPN Tunnel is required to verify connectivity through the tunnel.

Choose the interface that the VPN Tunnel has listed for the Local Subnet end-point, i.e. if the Left Subnet is 10.100.100.0/24 and eth1 has 10.100.100.1 as its IP Address, then choose Source Interface eth1.

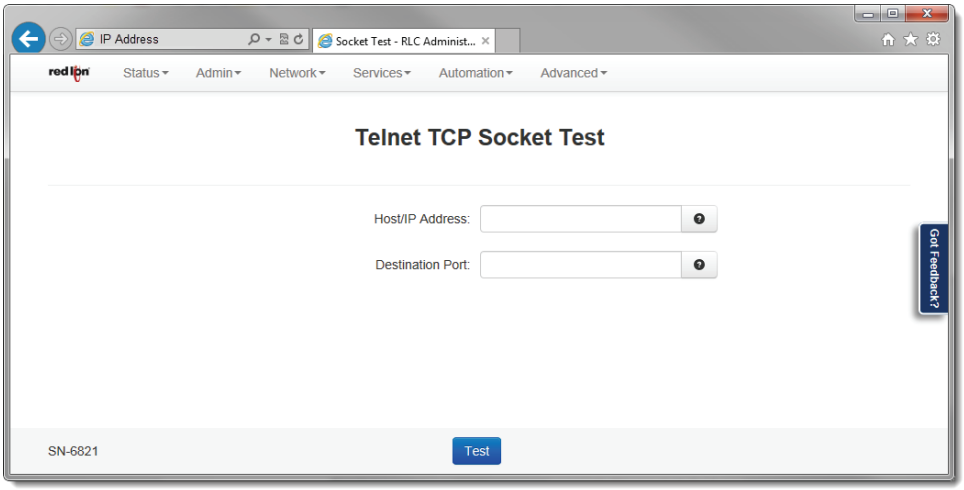
Specify a Host/IP Address at the head-end to Ping through the tunnel.

- Click on the Ping button to see the result.



3.2.3.3 Socket Test

The Socket Test menu item will allow you the “Telnet” to desired destination IP and Port addresses to verify the socket availability.



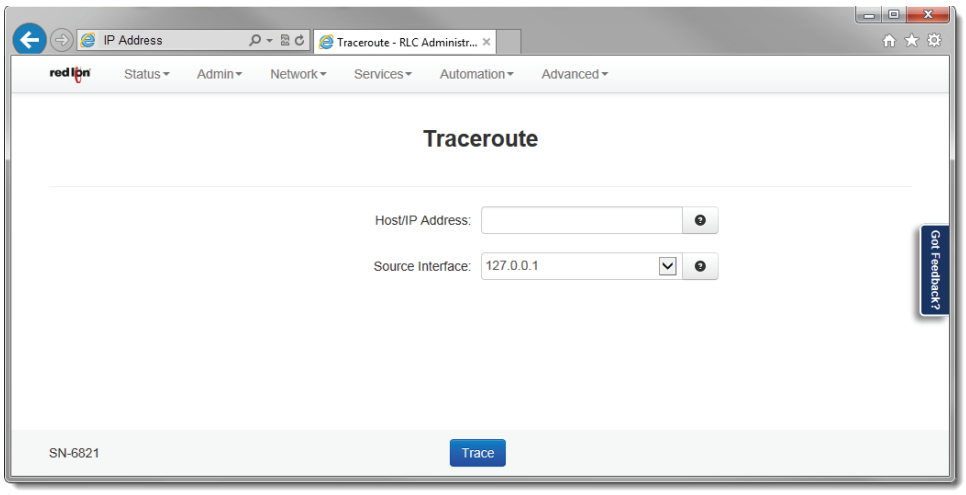
Host/IP Address field: Type in the IP Address or URL you wish to connect to via Telnet.

Destination Port field: Enter the Destination IP Address of the server to which you would like to connect.

- Click on the Test button at the bottom of the dialog window to proceed with the TCP socket test to verify socket availability.

3.2.3.4 Traceroute

The Traceroute menu item will allow you to watch the route taken through the Internet to the specified IP Address or URL.



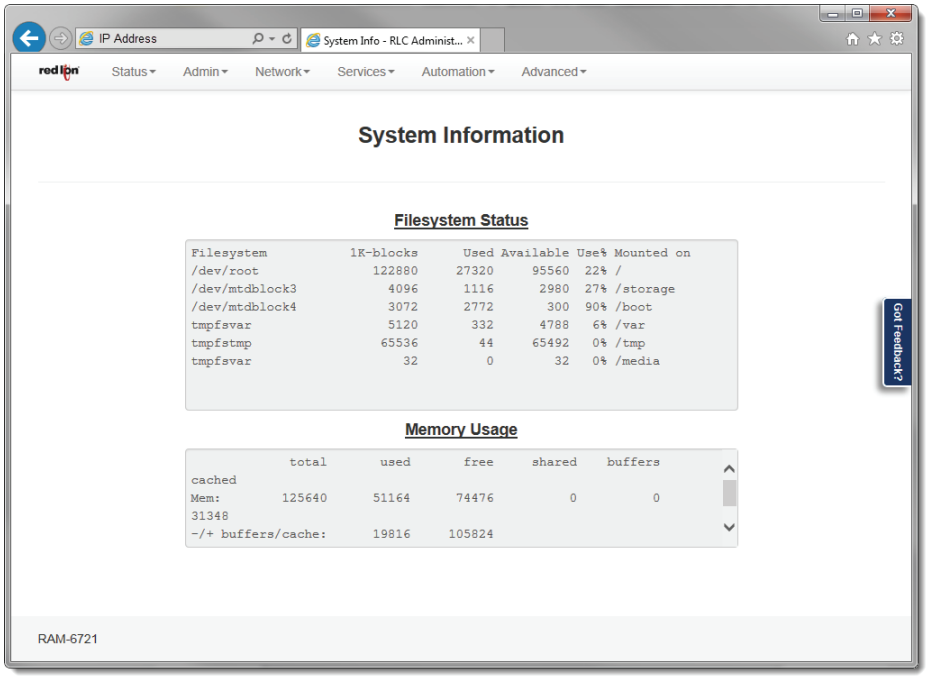
Host/IP Address field: Type in the IP Address or URL you wish to trace. It is recommended to start with a locally accessible IP address to confirm communications to an interface's local subnet. Then proceed to addresses on distant networks. You local default gateway is a good test, and this IP can be found in your routing table. A commonly available internet server available to test against is 4.2.2.2.

Source Interface field: Select the interface to be used from which to originate the Traceroute test. The recommended setting for this field is "Unspecified", as it will let the system choose the first interface found with a route to the destination.

- Click on the Trace button at the bottom of the dialog window and a table describing the Trace Route results will appear in the dialog window.

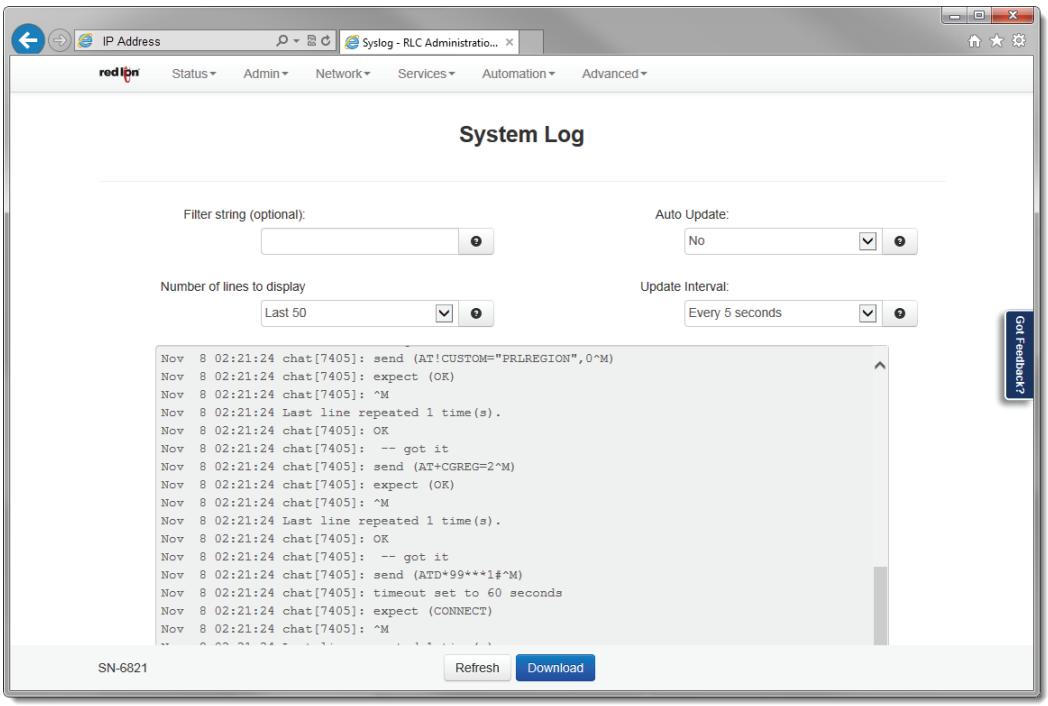
3.2.3.5 System Info

The System Info menu item will display the current usage of the file system in both the directory size and the memory utilization.



3.2.4 Syslog

The Syslog window will display the current log into the syslog of the Red Lion router.



Customize your search by configuring the following fields:

Filter String (optional): Enter a filter string in the space provided. Only lines containing the filter value(s) will be displayed via a GREP (Global Regular Expression Parser) style filter mechanism.

Auto Update: Select YES to enable automatic updating of the log file display. The update interval can be selected using the *Select Update Interval* option provided in the field below the *Auto Update* one. Manual updating is disabled while auto update is in effect. The current filter and maximum lines to be displayed will be used.

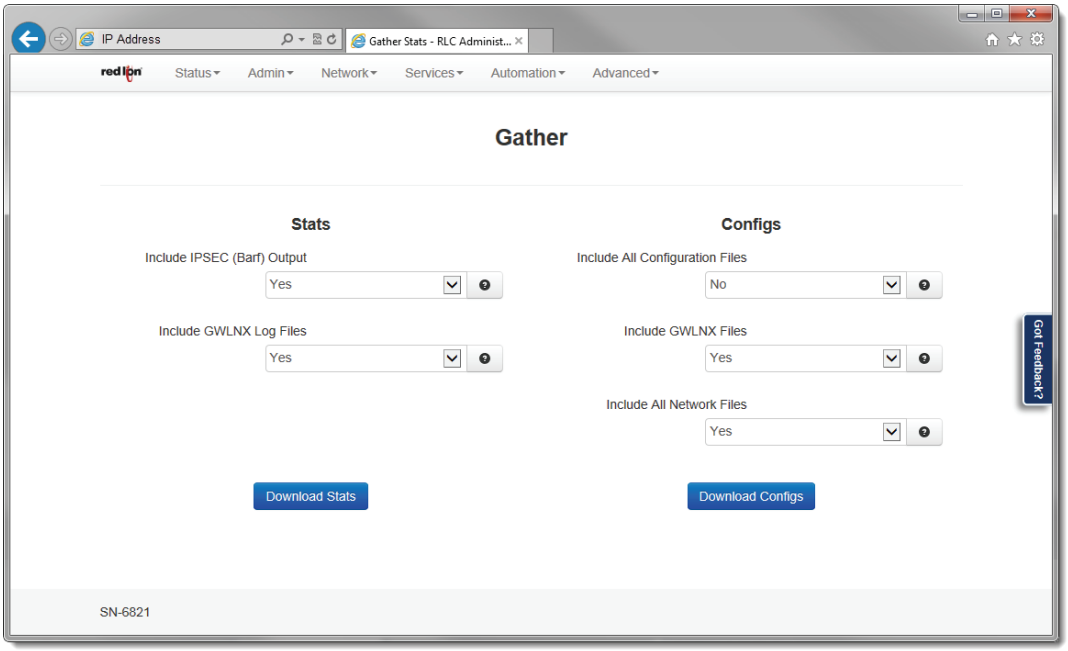
Number of lines to display: Select the number of lines to be displayed from one of the choices in the drop-down list provided.

Update Interval: Select how often you wish the update interval to be used when auto update is enabled.

Forward syslog to remote host: Select YES to enable forwarding of syslog messages to another host. The recommended setting for this field is NO.

- Click on the download button and the following window will appear prompting whether to save or open the file:

3.2.5 Gather Stats



Include IPSEC (Barf) Output: Select YES to include all IPSEC (Internet Protocol Security) debug information.

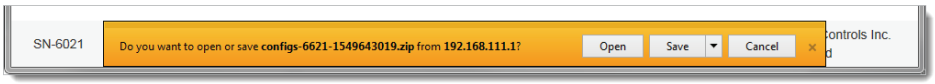
Include GWLNX Log Files: Select YES to include all GWLNX related logs. Choose YES if you are running GWLNX for protocol conversion. This will increase the size of the resulting .zip file.

Include All Configuration Files: Select YES to include ALL GWLNX protocol conversion related files. This included GWLNX application as well and will considerably increase the size of your resulting zip file. Note: Only choose YES for this option if directed by the Technical Support Staff.

Include GWLNX Files: Select YES to include all GWLNX configuration files. The recommended setting for this option is YES.

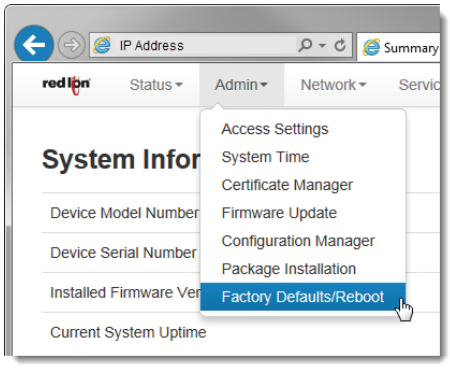
Include All Network Files: Select YES to include all networking related configuration files. If using “gatherconfigs” to clone a unit, note that this option will cause the network interfaces (Including static IP addresses) to be cloned as well. Note: If performing a gatherconfigs for review by technical support staff, please choose YES for this option.

- To create the download files for the Stats and/or Configs, click on the Download Stats and Download Configs buttons. The following pop-up will show up asking whether you want to open or save the file.



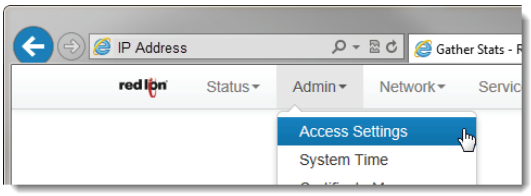
3.3 Admin Tab

The Admin Tab is where you configure web access methods, manage SSL/IPSEC certificates, set passwords, update firmware, manage configurations and set factory defaults.

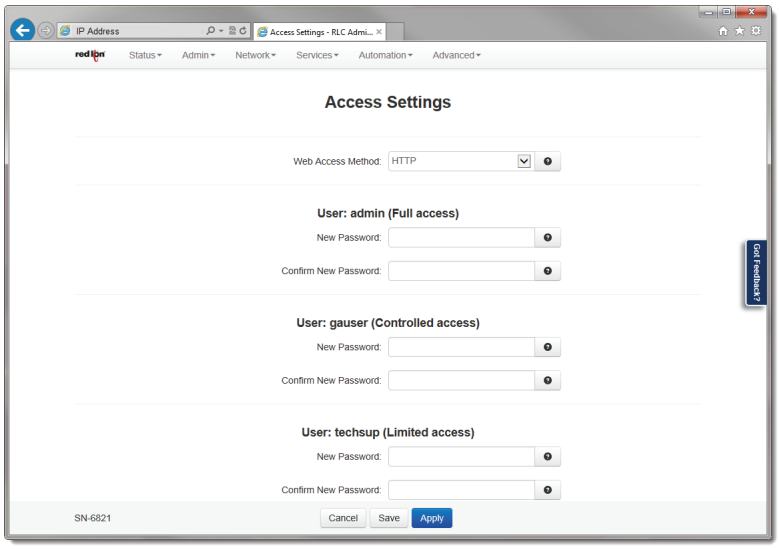


3.3.1 Access Settings

The “Access Settings” menu item allows you to change how the unit’s Web UI is accessed, either by HTTP or HTTPS. You can also change the passwords used to access the Web User Interface. For security purposes, it is recommended that the admin password be changed according to your internal policies.



- Click on the “Access Settings” menu item and the following window will appear.



Web Access Method: Select the method you would like to use to access the Web UI. You do not need to enter the password in order to change the access method. ***Note:*** The HTTP method can result in better performance and faster page load time; however, it is less secure than the HTTPS method, which uses data encryption to provide a secure connection.

User: admin (Full access)

New Password: Enter the new password in the "New Password" field. ***Note:*** For a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower case characters and numbers. *For security purposes, it is recommended that the admin password be changed according to your internal policies*.

Confirm New Password: Re-enter the password entered in the New Password field.

User: gauser (Controlled access)

New Password: Enter the new password in the "New Password" field. ***Note:*** For a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower case characters and numbers. *For security purposes, it is recommended that the admin password be changed according to your internal policies*.

Confirm New Password: Re-enter the password entered in the New Password field.

User: techsup (Limited access)

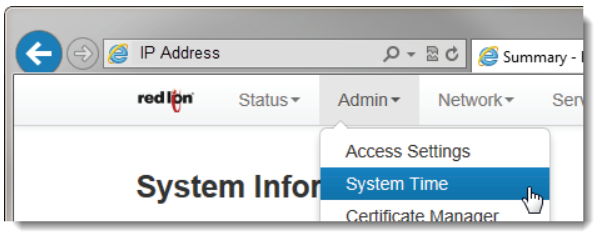
New Password: Enter the new password in the "New Password" field. ***Note:*** For a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower case characters and numbers. *For security purposes, it is recommended that the admin password be changed according to your internal policies*.

Confirm New Password: Re-enter the password entered in the New Password field.

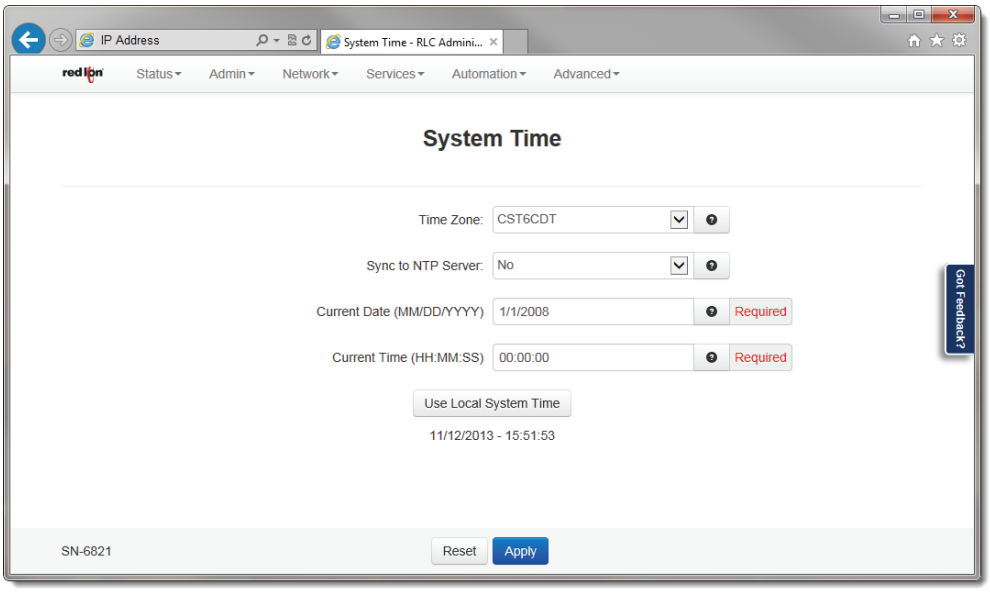
- Click on the "Save" button for changes to be saved without activating the interface, the "Apply" button will save your settings and apply them immediately. To revert to the previous settings, click on the "Revert" button.

3.3.2 System Time

The System Time menu item is used to configure the time zone on the Red Lion router to correspond to your location.



- Click on the System Time menu time and the following window will appear.



Time Zone: Select the time zone corresponding to your geographical location by choosing one of the values available on the drop down list provided.

To configure the date and time for your Red Lion router there are three options:

Option 1:

Sync to NTP Server: Select Yes to enable synchronizing the system clock to an NTP server.

Option 2 - Manual Configuration:

Current Date (MM/DD/YYYY) (Required): Set the Sync to NTP Server field to No and enter the Current Date using the shown format.

Current Time (HH:MM:SS) (Required): Set the Sync to NTP Server field to No and enter the Current Time using the shown format.

Note: The Hour field in on the 24-hour time clock, range 00-24. This page verifies that the month, day, year, hour, minute and seconds conform to expected inputs. For example, month range from 01-12, days range from 01-31 (checks for limit according to month, i.e. January has 31 days, February has 28 or 29 depending on year, etc.)

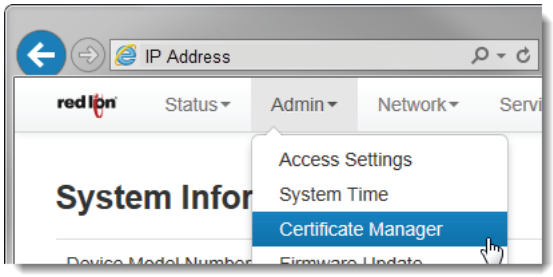
Option 3:

Use Local System Time: Set the Sync to NTP Server field to No and click on the Use Local System Time button. The local time as referenced from your browser is used to populate the settings.

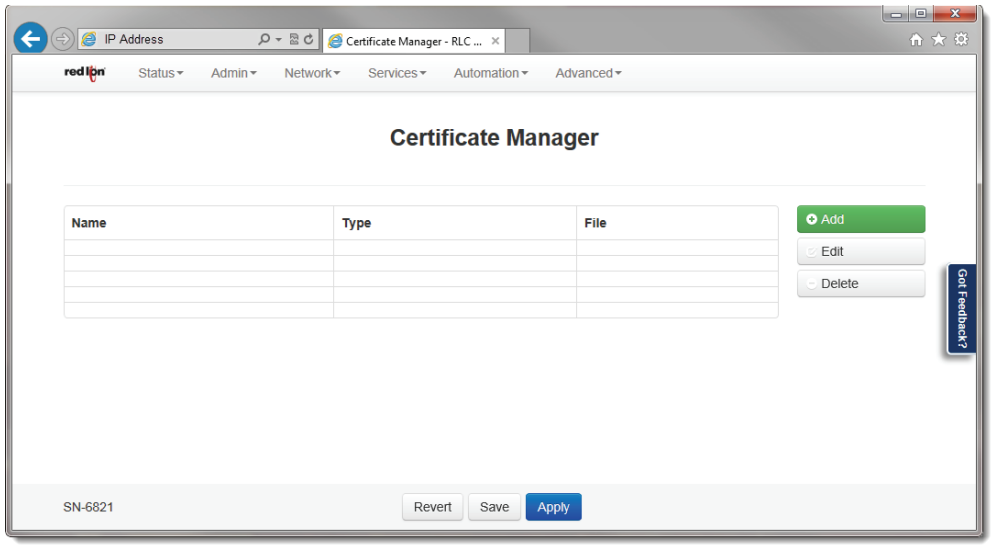
- Click on the Apply button to save your settings and apply them immediately. To revert to the previously saved defaults, click on the “Revert” button.

3.3.3 Certificate Manager

The Certificate Manager gives the option of adding a certificate, deleting or editing an existing one.

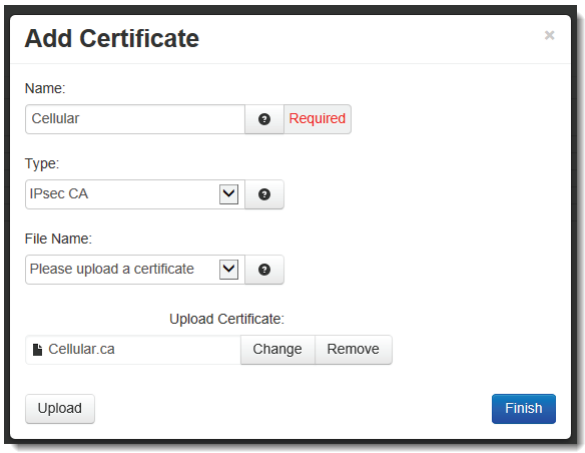


- Click on the Certificate Manager menu item and the following dialog window will appear:



To create a new certificate:

- Click on the Add button and the following dialog window will appear:



Name: Enter a descriptive name to be associated with the Certificate File to be uploaded. This name will be used later in fields where selection of a certificate is required. The descriptive name can contain only upper and/or lower case **letters** and **digits**.

Type: Select the type of certificate that you will be uploading. Each certificate is stored in a unique repository, depending on the service that will be using it. The certificate file name can contain only upper and/or lower case letters, digits, '-', '_' and must end with a .ca, .csr, .crt, .key or .pem.

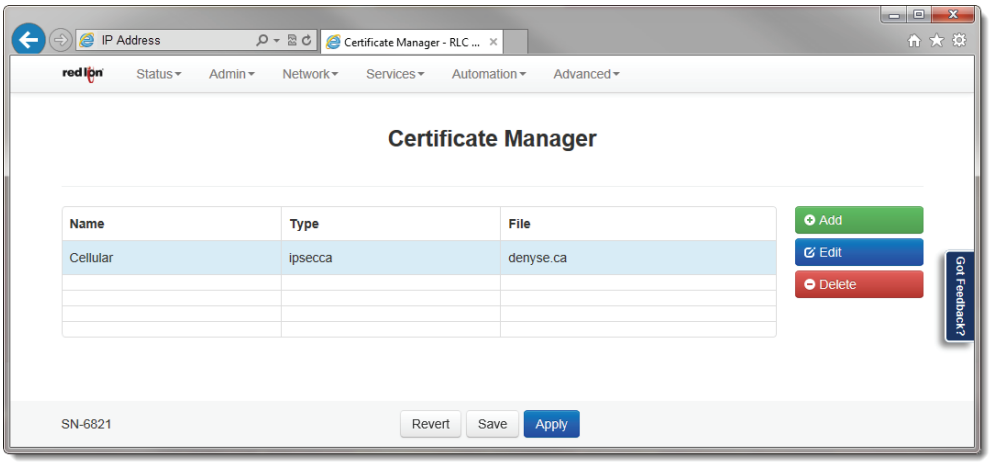
Possible choices include:

- IPsec Cert: This will specify a certificate to be used to authenticate a VPN connection. A server and client certificate will be required.
- IPsec Key: An RSA key must be provided for any client certificate uploaded. If this is signed with a password, that will need to be entered in the IPsec as well.
- IPsec CA: This specifies a Certificate Authority. Please include a CA valid for each signed certificate.
- SSL: This certificate will be available for SSL Connections as a Server Certificate, or a Client Certificate.
- SSLVPN: This certificate will be available for SSL VPN tunnels.

File Name: Once you have entered a value into the Name field, the Browse button will be enabled and can be clicked to select a file from your local system for upload. When a valid file name is selected, the Upload button is enabled and can be clicked to upload the selected file to the device. The certificate file name can contain only upper and/lower case letters, digits, '-', '_' and must end with a .ca, .csr, .crt, .key or .pem.

Note: SSL type certificates must include the key and cert portions, and the key must not be password encrypted.

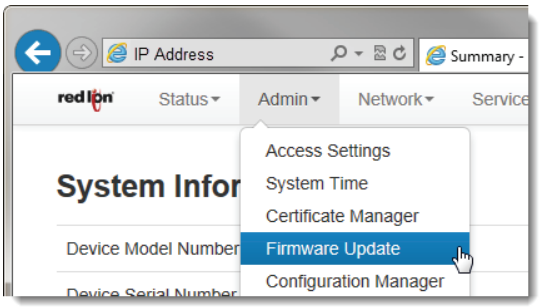
- Click on the Finish button and you will be directed to the Certificate Manager dialog window and the table will be populated with the entered data.



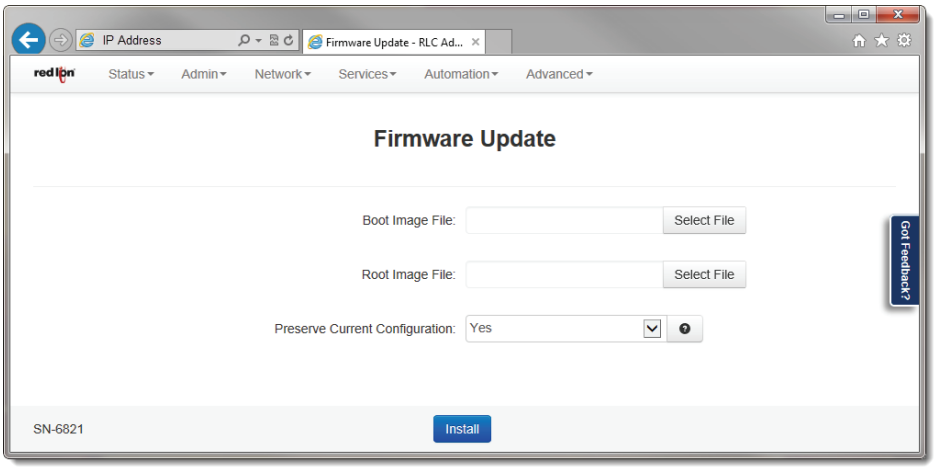
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the "Save" button for changes to be saved without activating the interface until you reboot the unit, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.3.4 Firmware Update

The Firmware Update menu item is used to upgrade the firmware of the Red Lion router.



- Click on the Firmware Update menu item and the following window will appear:



To upgrade the firmware of the Red Lion router:

Boot Image File: Select the file that will perform the Kernel update.

Root Image File: Select the file that will perform the system update.

Preserve current configuration: Select YES to save the device's current configuration and restore it after the firmware image is installed.

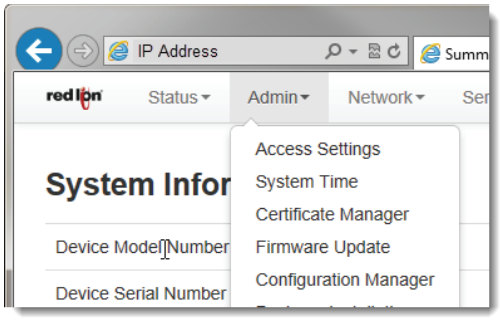
- Click on the "Install" button.

Note: This procedure could take anywhere from 6-10 minutes to complete.

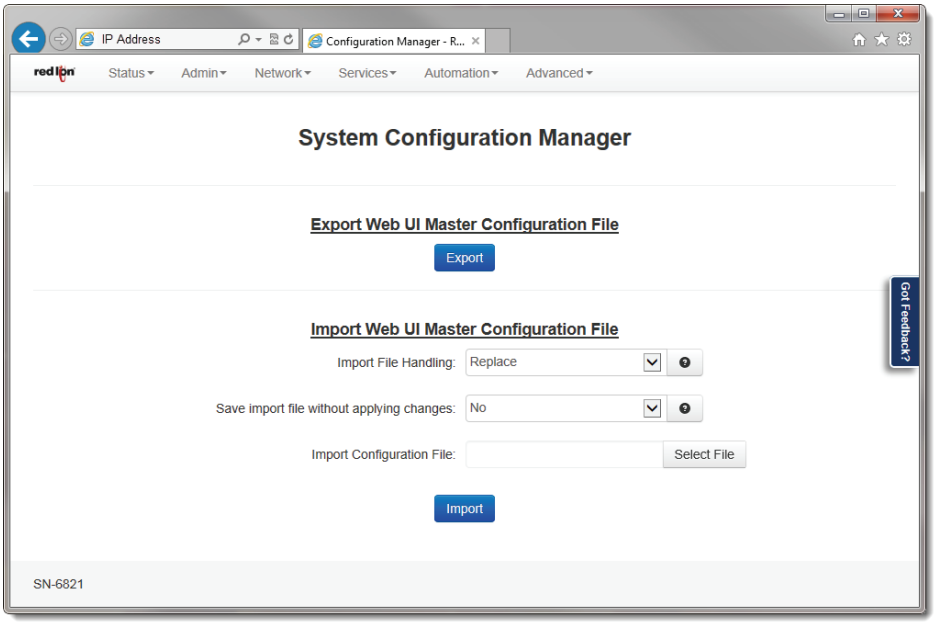
WARNING: It is important that the power to the unit is **not** interrupted at any time during the upgrade process, as this could cause the unit to become corrupt and require shipment back to the factory to correct.

3.3.4.1 Configuration Manager

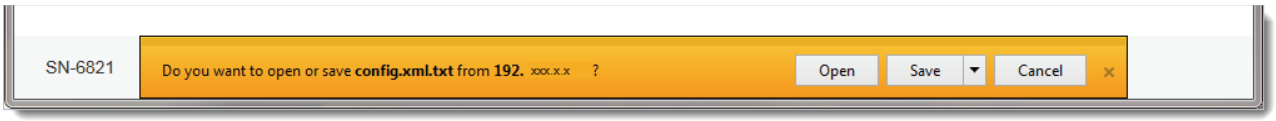
The Configuration Manager menu item saves a copy of the current system configuration, i.e., Export. This is useful when a confirmed good configuration is operational. A backup can be exported for use should the configuration become corrupt or re-configured in error.



- Click on the Configuration Manager menu item and the following window will appear:



Export Web UI Master Configuration File: To save a copy of the Red Lion router configuration, click on the "Export" button. The pop-up window below asking you to save or open the file will appear. Select the desired option.



Note: Please note the directory where the file was saved in order to retrieve it when needed to put the file back onto the Red Lion router.

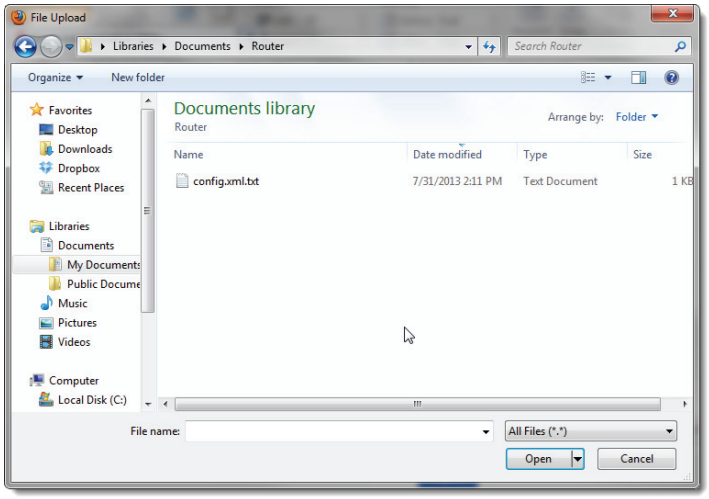
Import Web UI Master Configuration File: Set your importing defaults for the configuration file.

Import File Handling: Select Replace to completely replace the device configuration file with your import.

Save Import file without applying changes: If you want to save the new configuration without immediately applying it, simply select YES.

To apply the settings, you will need to visit the configuration page for each supported sub-system and click its Apply button. This is unusual, but useful for when you are importing a configuration from one unit to another and need to make additional settings before applying them.

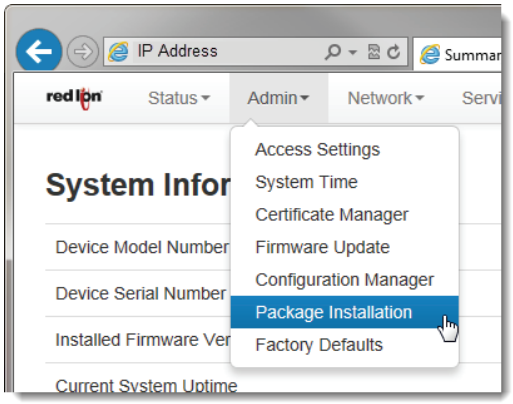
Import Configuration File: Click on the Select File button, and the dialog window below will appear.



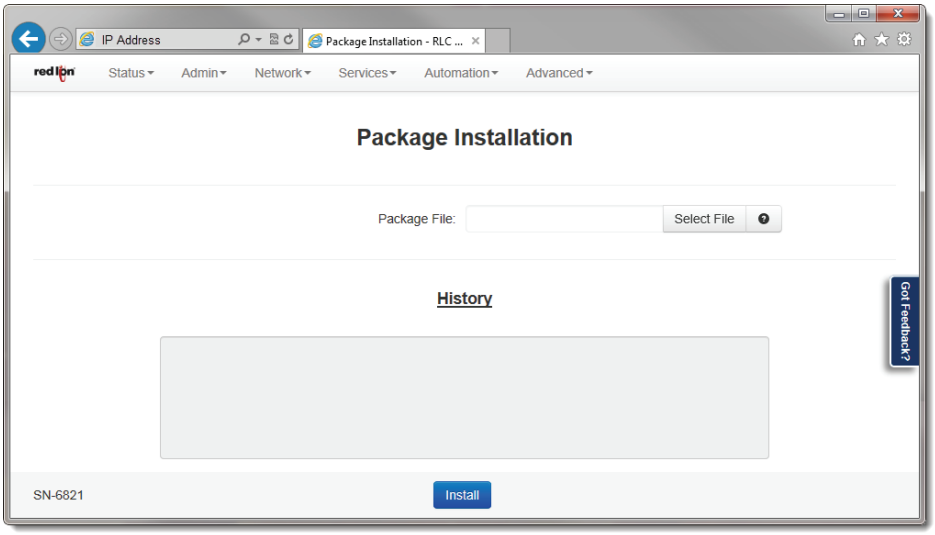
- Browse to the directory where the config.xml.txt file is located.
- Select the config.xml.txt file and click on the Open button to populate the Browse window. If needed, you can change the file or remove it from the field by clicking the appropriate button
- Click on the Import button. When import is complete, a table will appear at the bottom of the dialog window listing the modified files.

3.3.4.2 Package Installation

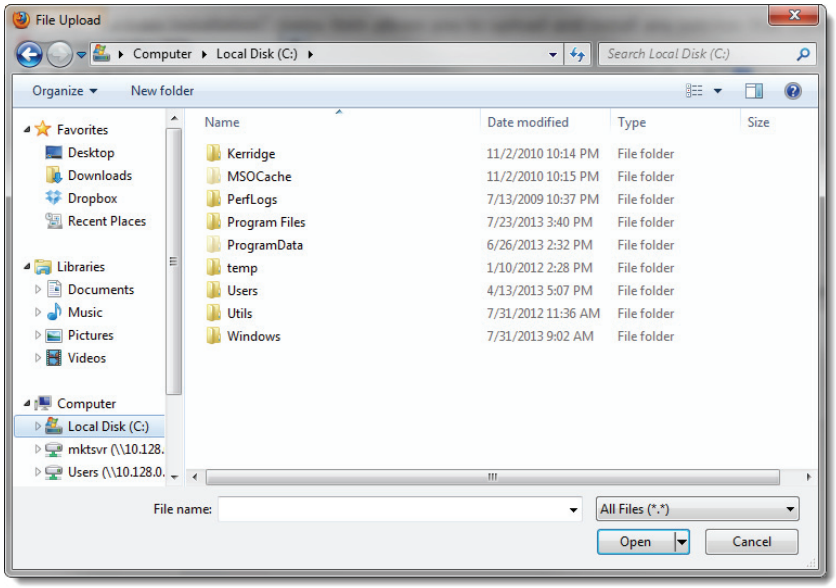
The Package Installation feature allows you to upload and install patches from Red Lion.



- Click on the Package Installation menu item and the following dialog window will appear:



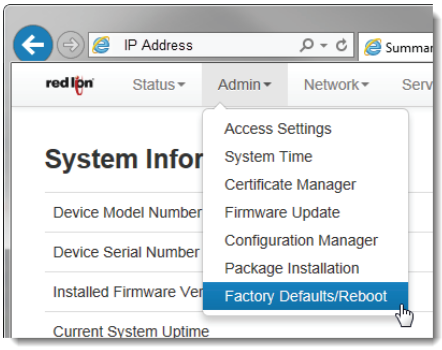
- In the Package File field, click the Select File button, and the following dialog window appear:



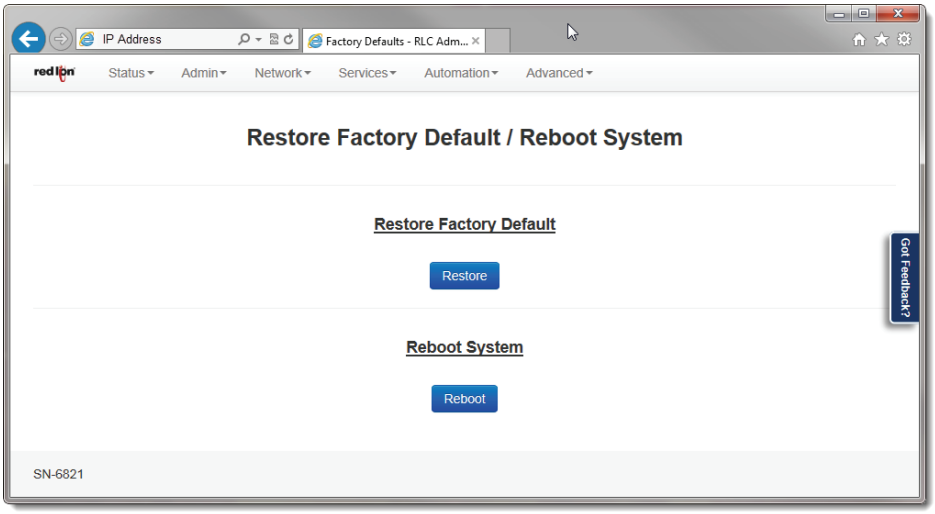
- Browse to the directory where the patch is located.
- Select the filename to select the file. Note: Be sure to use only genuine Red Lion provided packages in the form of filename.zip.
- Click on the Open button to populate the Package File field and click on the Install button. When install is complete, a table will appear at the bottom of the dialog window listing the modified files.

3.3.4.3 Factory Defaults/Reboot

The Factory Defaults/Reboot menu item allows you to restore the configuration back to factory default settings.



- Click on the Factory Defaults/Reboot menu item and the following window will appear:

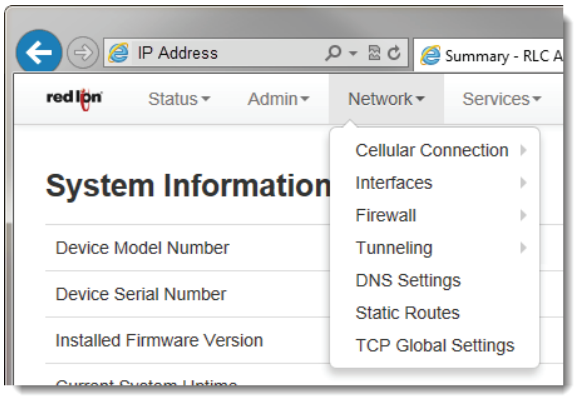


Restore Factory Default: Click on the Restore button to restore the factory default settings. A warning will appear, read through the information and click OK. The restore may take 2-5 minutes.

Reboot System: Click on the Reboot button to reboot the device. A warning will appear, read through the information and click OK. The reboot may take 2-5 minutes.

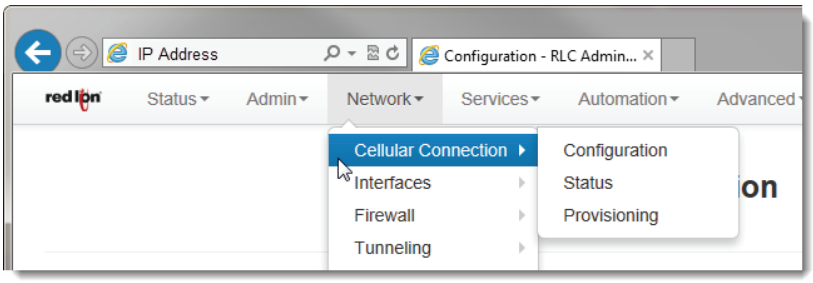
3.4 Network Tab

The Network Tab configures aspects of the Red Lion router affecting the networking functionality of the unit. From here you can configure the Cellular Connection (should the air card/SIM not be recognized at power up), Ethernet Interfaces, Firewall, Tunneling, DNS Settings, Static Routes and TCP Global Settings.



3.4.1 Cellular Connection

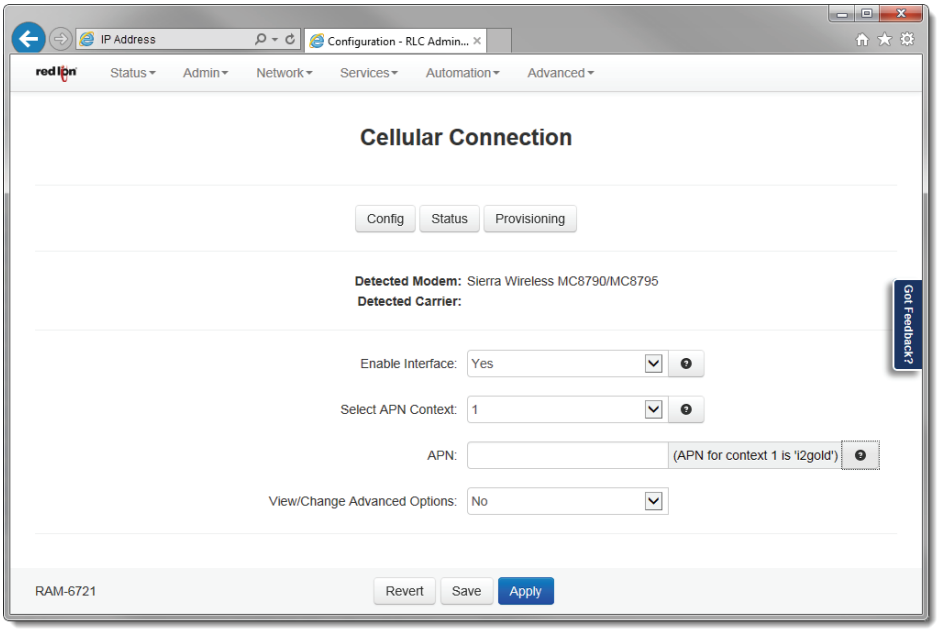
The Cellular Connection menu item is sub-sectioned into Configuration, Status and Provisioning. These options allow the user to configure/view the cellular information on unit.



3.4.1.1 Configuration

The Configuration menu item is used to make configuration changes to the cellular connection settings air on the Red Lion unit.

- Click on the Configuration menu item and the dialog window below will appear:



The Config, Status and Provisioning buttons are a quick way to navigate to the three (3) submenus of the Cellular Connection menu.

Enable Interface: Select Yes to enable the interface to become active after the new settings are applied and upon subsequent system start-up. Select No to disable the cellular interface and prevent the cellular radio from attempting to establish a network connection.

Select APN Context: Select the desired APN Context from the provided drop-down. This information should have been given to you by your service provider when service was established.

APN: Enter the APN used to access your cellular wireless data service in this field. **Note:** Entering an APN value in this field will overwrite any APN stored in the modem for the selected context.

View/Change Advanced Options: Selecting Yes will enable the additional fields listed below.

User Name: Enter the user name assigned to you by your cellular wireless data plan provider. This information should have been given to you by your service provider when service was established.

Password: Enter the password assigned to you by your cellular wireless data provider. This information should have been given to you by your service provider when service was established.

Confirm Password: Re-enter the password entered in the password field, exactly as typed before.

Dial String: Enter the dial string used to access your cellular wireless data service in this field. This information should have been giving to you by your service provider when service was established. The dial string must be entered in the form of an AT command string, such as ATDT#777. The recommended setting for this field is to leave it blank.

SIM Unlock PIN Code: Enter the 4 digit SIM Unlock PIN code here. Entering the wrong value multiple times may cause your SIM to become unusable and require service by your carrier. If you have previously entered this value, but it is now blank, the PIN was probably rejected by the SIM. Rejected PIN codes are cleared so that they are not attempted multiple times. Use this option with caution.

RF Radio Region: This option chooses the RF bands to scan for available towers, and sets the PRL Region option in the module if applicable.

0 - Default:

Band Group 0 - G900 G1800 W2100 W800

Band Group 1 - G1900 G850 W1900 W850

1 - Europe/Rest of the World:

Band Group 0 - G900 G1800 W2100 W800

Band Group 1 - G1900 G850 W1900 W850

2 - North America:

Band Group 0 - G1900 G850 W1900 W850

Band Group 1 - G900 G1800 W2100 W800

3 - Australia:

Band Group 0 - G900 G1800 W850 W2100 W800

Band Group 1 - G1900 G850 W1900

4- Japan:

Band Group 0 - G900 G1800 W2100 W800

Band Group 1 - G1900 G850 W1900 W850

Select Cellular Network Speed: Select the connection speed to be used for the cellular modem connection from the drop down list provided. Possible values include: Auto, High and Low. The recommended setting for this field is Auto.

Cellular MTU: Enter the MTU size you desire to use. In computer networking, the maximum transmission unit (MTU) of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc.). Standards (Ethernet, for example) can fix the size of an MTU; or systems (such as point-to-point serial links) may decide MTU at connect time. A larger MTU brings greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation.

However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency. For example, a 1500-byte packet, the largest allowed by Ethernet at the network layer (and hence over most of the Internet), ties up a 14.4k modem for about one second.

The recommended setting for this field is 1500.

Sync Time: This option will attempt to take the local time as reported by the cellular tower, and set the unit's system time to match. The recommended setting for this field is Yes, unless another method of time Sync, such as NTP is being used.

Choose Connection Behavior: In Persistent mode, the unit will always attempt to maintain a cellular connection with the carrier's network. In On-Demand mode, the connection to the cellular network will only be attempted when packets are destined to leave the wireless interface. In addition, after a period of Idle Time, the connection will terminate.

Persistent mode has the potential to use more bandwidth in a limited data plan meant for fallback. For this reason, On-Demand is commonly chosen for an environment using an ethernet connection as a primary interface, while IP Fallback is used to bring up the secondary wireless connection as a backup. Modern cellular connections use idle states in on-board radios to often negate the need for an On-demand option.

Maximum Receive Idle Time (rxidle): Enter the number of seconds the connection may be allowed to remain “idle” or “unresponsive” (no data received) before closing the connection. If packets are leaving the interface, but no return packet is received for the specified time, then the connection is reset. This can be useful for detecting an unresponsive situation where the network is down, the modem is in an unknown state, or other low level error may have occurred.

Note: *If the normal usage of the device regularly has packets leaving the unit with no expected response, then premature disconnections may result. Outgoing UDP packets with no expected response may be normal operation, yet will trigger this disconnection and reset.*

The recommended setting for this field is 0 to turn off. The recommended value to enable this feature is 150 seconds (2.5 minutes).

User Default Route: This field allows you to choose to have the default route for the Red Lion router to be the cellular connection when it is connected, or to designate an Ethernet port as the default route. Select Yes to have the cellular connection use the default route once it is connected.

Use Peer DNS: Select Yes to have the cell connection accept DNS information from the peer device to which it is connected.

Auto add SNAT rule: When turned on, this option runs a script which, when a celluar connection comes up, will add a firewall rule which forces a packet to source the IP address that the PPP interface receives from the remote ISP.

Normally recommended for a wireless interface which has a static IP (never changes). Can sometimes cause problems with dynamic IPs.

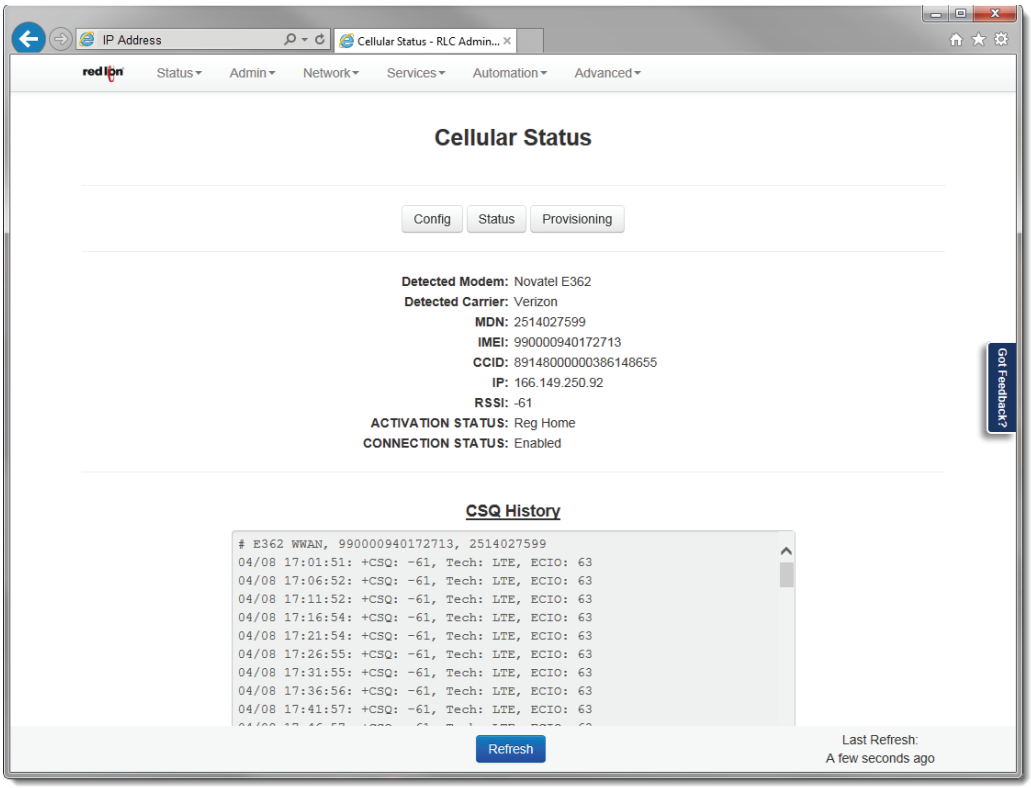
The recommended setting for this field is NO.

Enable Custom AT and PPP Commands: Custom AT and PPP commands are for advanced users and configuration. This option should **not** be enabled or used except under the direction of Red Lion Technical Support. Enabling and entering items into this option can cause your Cellular modem’s connection to fail. The recommended setting for this field is No.

- Click on the “Save” button for changes to be saved without activating the interface, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

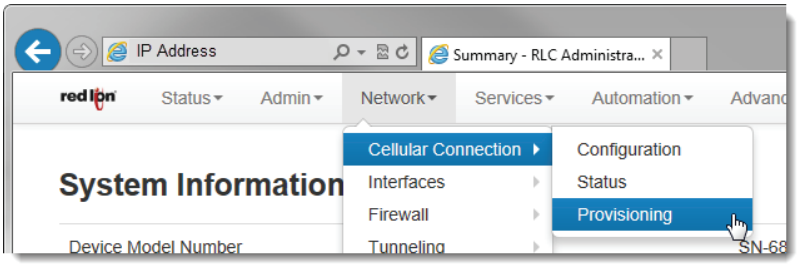
3.4.1.2 Status

The Status menu item will bring up a dialog window which displays the status of the cellular connection. From here, you can get information such as the type of modem, carrier, MDN, IMEI, ESN, IP, RSSI, Activation Status, Connection Status, CSQ Status and Card Stats.

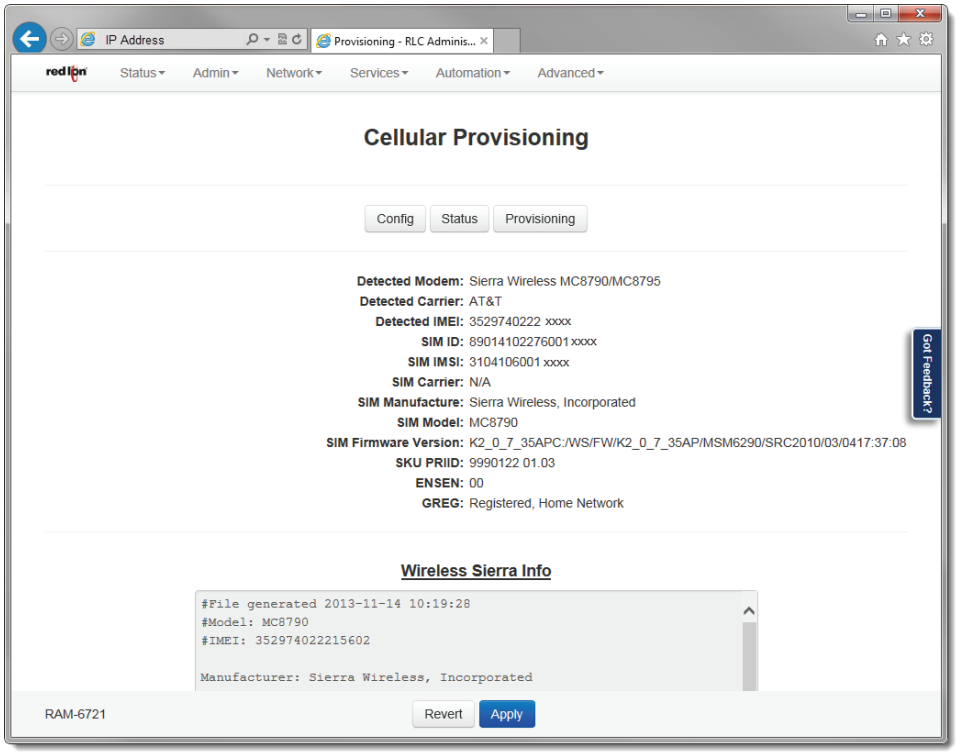


3.4.1.3 Provisioning

The Provisioning menu displays carrier specific information that may be useful when initially provisioning your device with a new carrier.



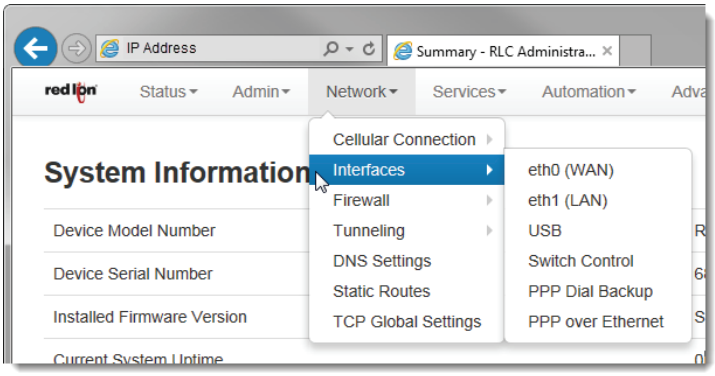
- Click on the Provisioning menu item. If a cellular connection is found, the following window will appear with the information about the modem in the upper window:



Note: If the cellular SIM is not recognized, go to the Configuration dialog window and enter the required data (see section 3.4.1.1).

3.4.2 Interfaces

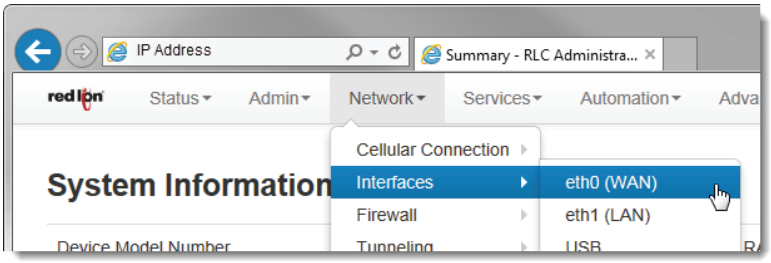
The Interfaces menu allows the administrator to configure the Ethernet ports of Red Lion routers to incorporate within their existing nework topology.



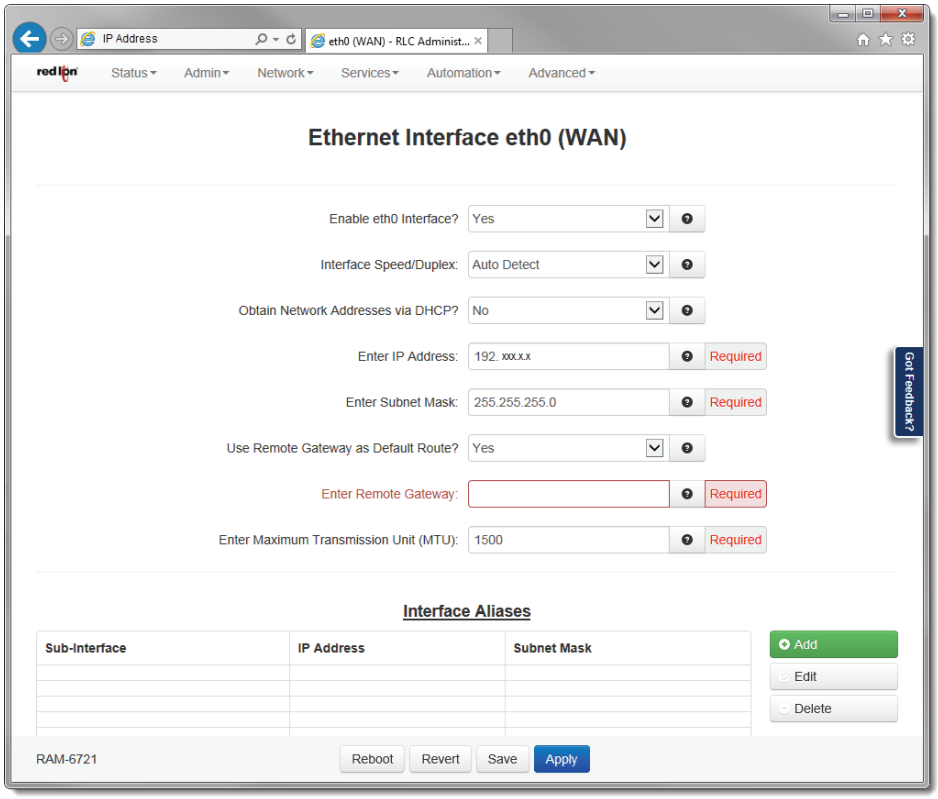
Interfaces available may include eth0 (WAN), eth1 (LAN), and USB. These will only be present if your hardware supports these interfaces. These ports are ‘auto-sensing’, allowing for greater flexibility.

3.4.2.1 eth0 (WAN) and eth1(LAN) - (Internet Interfaces)

The configuration of the Ethernet ports is the same for eth0 and eth1, therefore this section will only reference the configuration of “WAN”/’eth0’. Please refer to this section when configuring “LAN”/’eth1’.



- Click on the “eth0 (WAN)” menu item and the following window will appear:



Enable eth0 Interface: This field determines if the specified Ethernet port is enabled, allowing the administrator to disable the port if necessary.

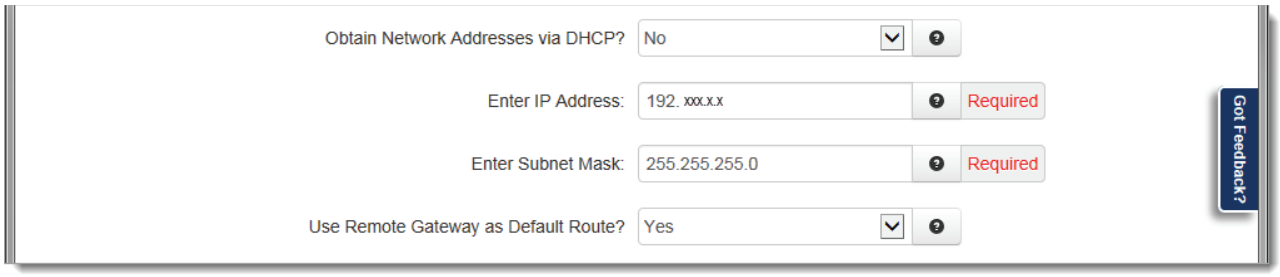
Interface Speed/Duplex: Select the Speed and Duplex to be used for the physical interface. The recommended setting for this field is Auto-Detect.

- Auto Detect: Use the ‘best negotiated’ speed and duplex. (default)
- 10Mbps/Half: Force the interface to 10 Mbps and half-duplex.
- 100Mbps/Half: Force the interface to 100 Mbps and half-duplex.
- 100Mbps/Full: Force the interface to 100 Mbps and full-duplex.

Note: An incorrect ‘forced’ setting will result in communication failure for this interface.

Obtain Network Addresses via DHCP: Select ***Yes*** to allow the interface to obtain address information via a DHCP server. The device will obtain its IP address, netmask and remote gateway and optionally, use the remote gateway as the default route. It can also obtain DNS server address via DHCP.

Select ***No*** to prevent the interface from obtaining address information via a DHCP server. You will be required to enter an IP address, netmask and remote gateway addresses. DNS information can be provided by navigating to Network -> DNS Settings.



Enter IP Address: This field appears when ***No*** is selected for "Obtain Network Addresses via DHCP". Specify the IP Address to be assigned to the Ethernet port when a 'Static' IP Address configuration is selected. This field will not be visible or accessible when a 'Dynamic' IP address configuration is selected, as the DHCP server will provide the Red Lion router with the IP address that it should use. This is a required field.

This address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the enter ***Subnet Mask*** field and must not conflict with any other device on the target network.

The IP address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.3, then the range of valid addresses is 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the network and 192.168.1.255 is the value reserved for the broadcast address.

Enter Subnet Mask: Enter the desired Netmask for the interface in the field provided. This field is only available when "Obtain Network Addresses via DHCP" has been set to ***No***.

Your Network Administrator should be able to provide an appropriate value for this field. This value determines the valid range of IP addressed allowed in the ***Enter IP Address*** field.

Use Remote Gateway as Default Route: Select Yes to use this interface as the default route. If **Obtain Network Addresses via DHCP** is set to Yes, then the interface is configured to obtain its address information from a DHCP server, and will use the gateway address provided by the server as the default route. If **Obtain Network Addresses via DHCP** is set to NO, then the IP Address of the remote gateway will be required to be entered in the Enter Remote Gateway field.

Note: On devices with multiple interfaces, if may be possible for this setting to be made multiple times. When the Web UI is used to configure an interface, the last settings applied are the ones which take precedence. When a device reboots, the last interface to become active takes precedence. For devices with interfaces which activate/deactivate dynamically (cellular connections, fall-back, etc.), the current interface activated takes precedence.

Use Peer DNS: Select **YES** to allow the interface to obtain DNS Server settings via DHCP. This field is only available when **Obtain Network Addresses via DHCP** has been set to **YES**. Select **NO** to allow the interface to use the DNS settings from the **Networking -> DNS Settings** screen. The recommended setting for this field is YES.

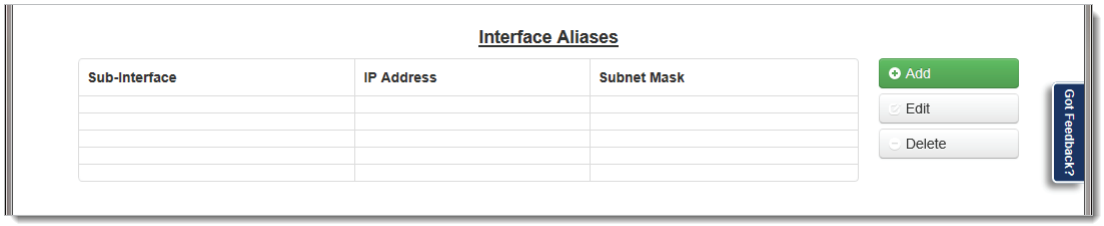
Enter Remote Gateway: Enter the IP Address for the gateway device in the field provided. This field is only available when **Obtain Network Addresses via DHCP** has been set to **NO**. This field is required if Use Remote Gateway as Default Route is set to Yes.

A gateway is a device (typically a router) used to gain access to another network. For example, if a device is attached to a LAN whose network address is 192.168.1.0 with a netmask of 255.255.255.0, then it can communicate directly with any other device on that network with a range of addresses of 192.168.1.1 through 192.168.1.254 (with 192.168.1.255 reserved for broadcast). An address outside of that range is on a different network which would need to accessed indirectly through a router and that router would be the gateway to the network on which the remote target device resides, so to communicate with it would mean sending and receiving via the gateway device. This also requires either defining a static route (defined through the **Network→Static Routes** screen) via that gateway or making it the default route (by setting **Use Remote Gateway as Default Route** to Yes.

Your Network Administrator should be able to provide an appropriate value. The address must be one within the valid range for the network.

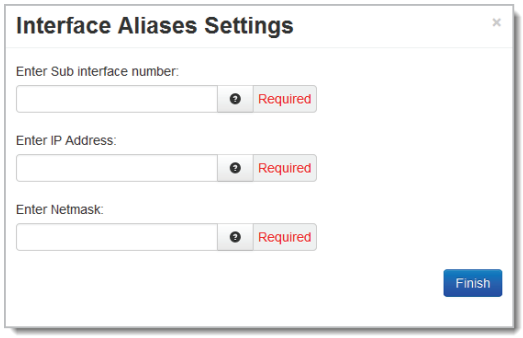
Enter Maximum Transmission Unit (MTU): Enter the desired MTU size. In computer networking, the **maximum transmission unit** (MTU) of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc). Standards (Ethernet, for example) can fix the size of an MTU; or systems (such as point-to-point serial links) may decide MTU at connect time. A larger MTU brings greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvements in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation. However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and layer (and hence over most of the Internet), ties up a 14.4k modem for about one second. The recommended setting is 1500.

Interface Aliases: Sub-interfacing is essentially the segmenting of a single wire, or port, into multiple IP networks. Instead of subnetting and routing, you can create a sub-interface and then set it up as you would a standard Ethernet interface.



To configure a sub-interface:

- Click on the Add button and the following pop-up window will appear:

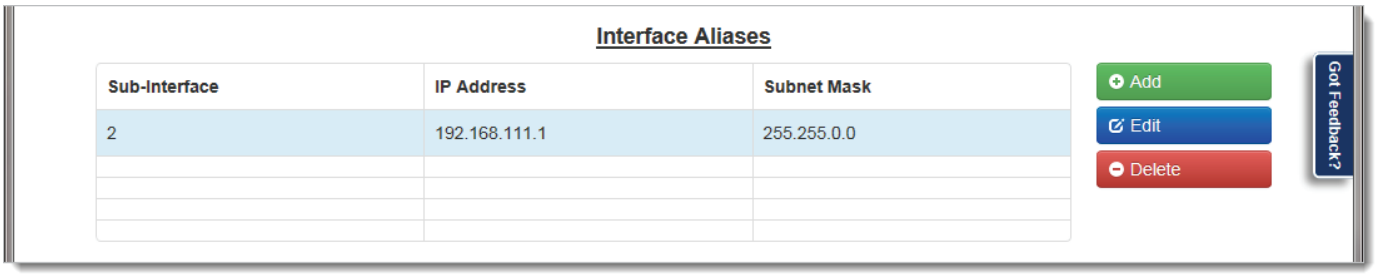


Enter Sub interface number (Required): This field is where you enter the sub interface number. The valid range is 0-99, and each aliased interface must be uniquely numbered. The final sub interface name will then be in the form **ethx:y** where **x** is the root interface number and **y** is the sub interface number. Your Network Administrator should be able to provide guidance as to an appropriate value.

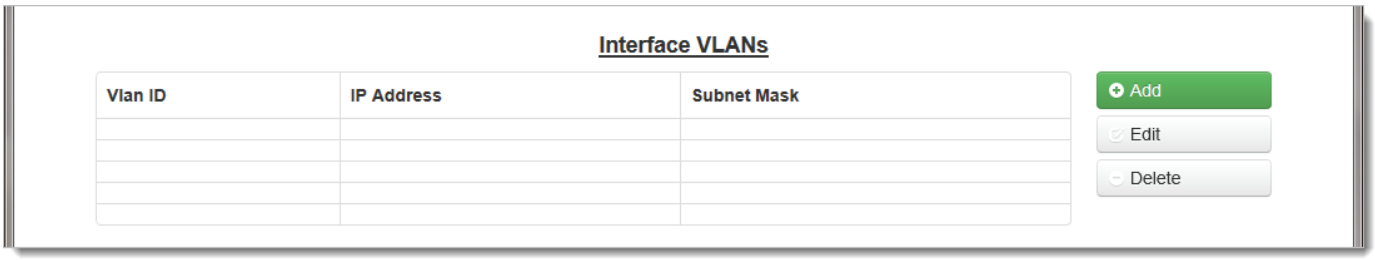
Enter IP Address (Required): This field specifies the IP Address of the sub interface. This address should have been provided by your Network Administrator.

Enter Netmask (Required): This field specified the netmask to be assigned to the sub interface. You Network Administrator should be able to provide an appropriate value.

- Click on the Finish button and you will be directed to the Ethernet Interface dialog window and the Interface Aliases table will be populated with the entered data.

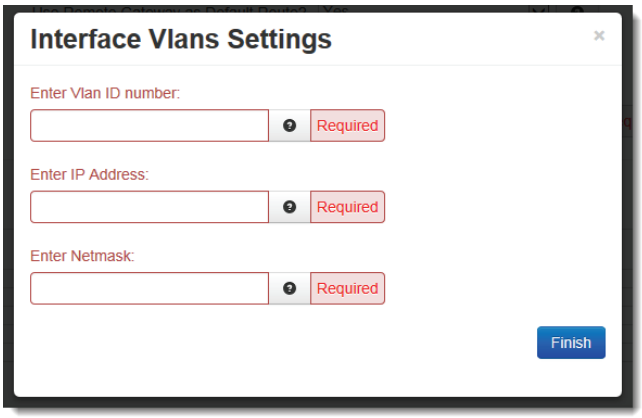


Interface VLANs: Sub-interfacing is essentially the segmenting of a single wire, or port, into multiple IP networks. Instead of subnetting and routing, you can create a sub-interface and then set it up as you would a standard Ethernet interface.



To configure an Interface VLAN:

- Click on the Add button and the following pop-up window will appear:

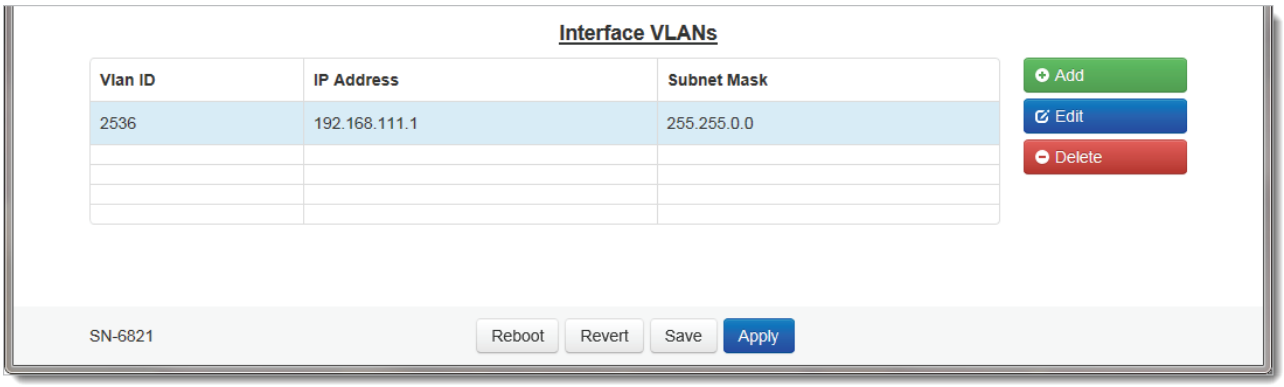


Enter Vlan ID number (Required): Enter the desired Vlan ID interface number in the field provided. The valid range is 0-4096 and each interface must be uniquely numbered. The final Vlan ID will then be in the form **ethx.y** where **x** is the root interface number and **y** is the vlan ID number. Your Network Administrator should be able to provide guidance as to an appropriate value.

Enter IP Address (Required): Enter the desired interface IP Address into this field. This address should have been provided by your Network Administrator.

Enter Netmask: Enter the desired Netmask for the Vlan interface in the field provided. You Network Administrator should be able to provide an appropriate number.

- Click on the Finish button and you will be directed to the Ethernet Interface dialog window and the Interface Aliases table will be populated with the entered data.



Reboot: Will restart the system and apply all the settings upon reboot.

Revert: Will revert the settings in the dialog window back to the previous saved settings.

Save: The interface will not be activated or deactivated until the device is rebooted. This allows for other configuration changes to be made to the device which can be committed at a later time.

Apply: The current settings will be saved and the interface will either be activated or deactivated immediately. If the interface was already active, then it will be deactivate and reactivated using the configured settings just saved. If you were connected to the Web UI via this interface, an attempt will be made to re-connect to it using the new settings, when possible.

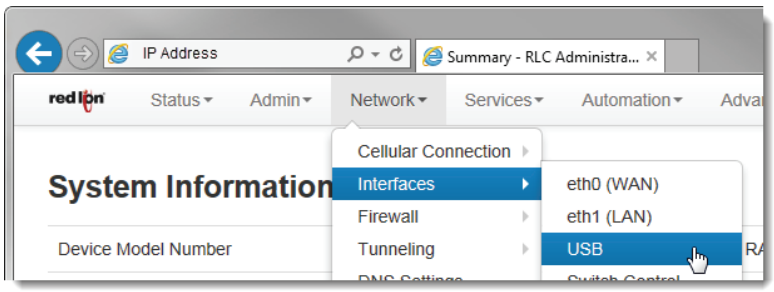
Applying new settings to the interface may result in disconnection, requiring reconnection using alternate methods.

Incomplete or incorrect network settings could render the device incommunicable and may require being able to connect either to the device directly or via the network to which it is attached.

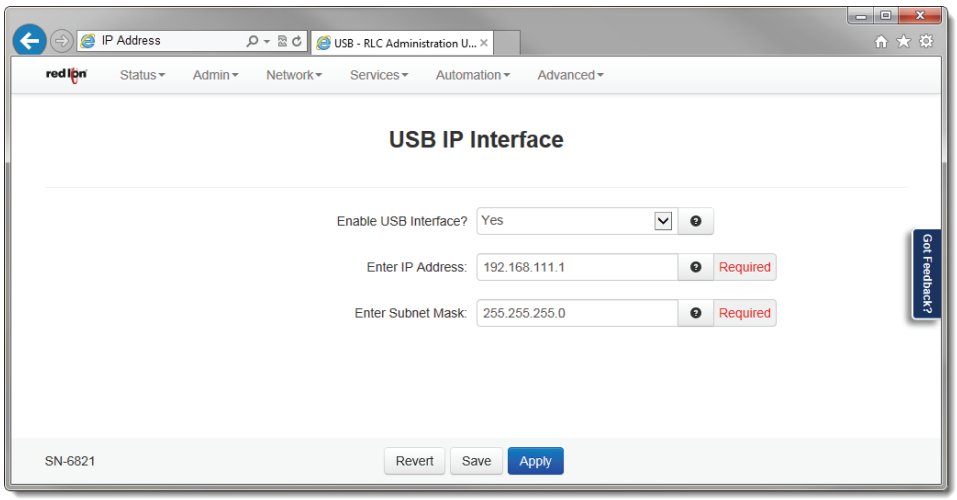
Note: *To work with the eth1 Interface, follow the steps documented for eth0.*

3.4.2.2 USB

The USB interfaces menu item allows the administrator to configure the USB port of the Red Lion routers to meet their needs. The default address is set for 192.168.111.1 with the subnet mask of 255.255.255.0



- Click on the USB menu item and the following dialog window will appear:



Enable USB Interface: Select ***YES*** to enable the USB interface. The recommended setting for this field if YES if using this interface.

Enter IP Address: Enter the desired interface IP address in this field. The IP Address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.3, then the range of valid addresses is 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the network and 192.168.1.255 is the value reserved for the broadcast address.

The IP address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the **Enter Subnet Mask** field and must not conflict with any other device on the target network.

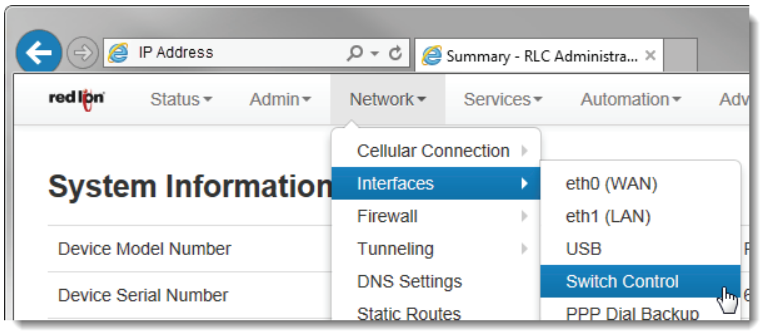
Enter Subnet Mask: Enter the desired Netmask for the interface in the field provided.

Your Network Administrator should be able to provide an appropriate value. This value determines the valid range of IP addresses allowed in the **Enter IP Address** field.

- Click on the “Save” button for changes to be saved without activating the interface, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

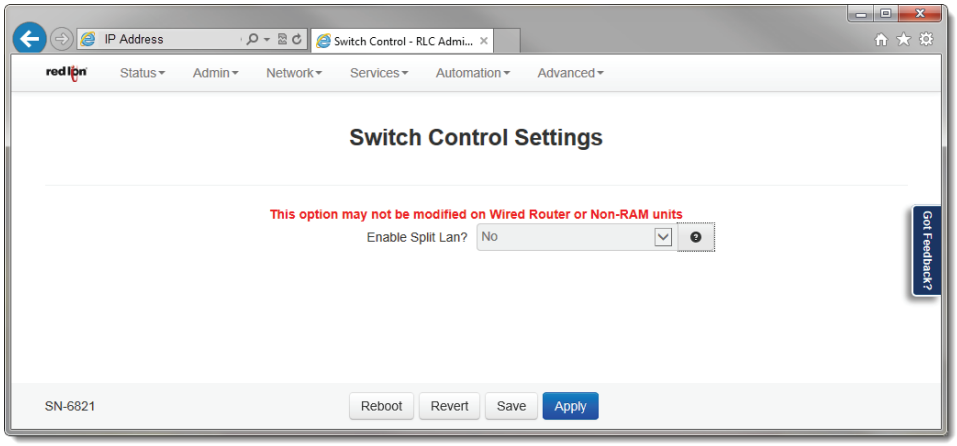
3.4.2.3 Switch Control

The purpose of the Switch Control function is to create a WAN/LAN separation This gives the user the ability to create a divided network with additional capabilities. This option only applies to units with the 5 port unmanaged switch (6x21).



Switch Control Settings

Enable Split Lan: This will alter the switch port allocations. When disabled, all switch ports 1-5 will be treated as a single LAN. This will be configurable as eth0 and will default to being a firewall trusted/internal interface.



When enabled, port 5 will be divided out as a WAN port, eth0 (firewalled as external/untrusted). Ports 1-4 will be an internally trusted LAN (eth1).

Warning: When switching modes, your firewall interface tables will be rebuilt and may need any custom changes reapplied. In addition, a USER INITIATED reboot is required to complete the mode switch.

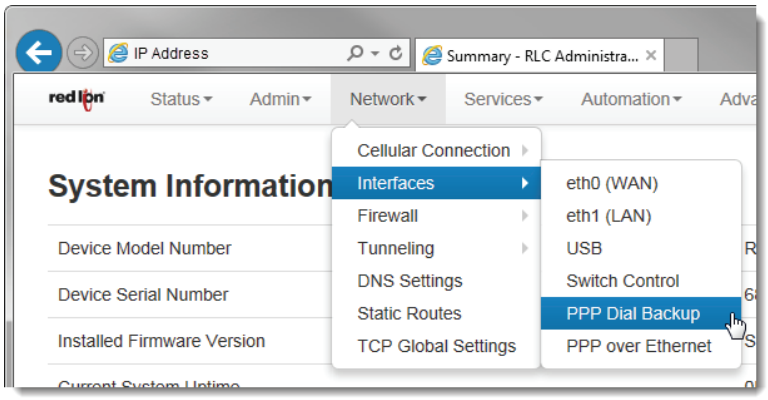
Warning: When enabling switch mode, current ethernet settings (eth0) will apply only to the single WAN port. On the front of the unit, this may be shown as <Port 5> under the power connector. The remaining four ports will be configured as a LAN (eth1).

Please check your Ethernet connections to make sure that the new settings will not conflict with previous network configurations. You may need to revisit your Untrusted/Trusted interface lists in the **Firewall -> General Settings**, as these will revert to new defaults (eth0 will be firewalled as Untrusted!). After Apply is clicked and you check firewall/ethernet configurations, a reboot is required to complete this process.

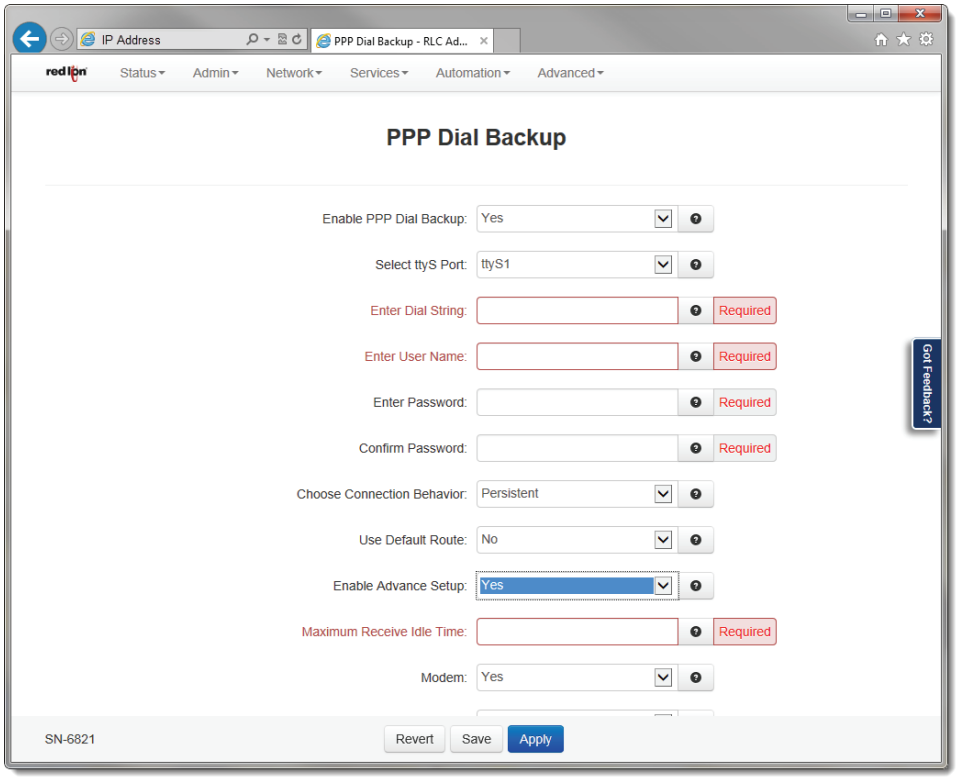
- Click on the “Save” button for changes to be saved without activating the interface, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.2.4 PPP Dial Backup

The PPP Dial Backup menu item is used to configure the capability of an alternate connection by dialing into an ISDN should the primary router get interrupted.



- Click on the PPP Dial Backup menu item and the following dialog window will appear:



Enable PPP Dial Backup: Select ***YES*** to turn on the PPP Dial Backup and ***NO*** to turn off PPP Dial Backup.

Select ttyS Port: Select the ttyS port on which the modem is attached. For an external modem connected to a serial port, use the port name as labeled on the unit. For an internal modem, a common setting is ttyS3.

Enter Dial String (Required): Enter the phone number of the peer/ISP to dial.

Enter User Name (Required): Enter the name used for authenticating the local system to the peer. Please consult your ISP for these values.

Enter Password (Required): Enter the password to use for authenticating with the peer. Please consult your IPS for these values.

Confirm Password (Required): Re-type the password entered in the Enter Password field.

Choose Connection Behavior: In Persistent mode, the unit will always attempt to maintain a constant connection to the POTS network. In On-Demand mode, the connection to the POTS network will only be attempted when packets are destined to leave the modem's PPP interface. In addition, after a period of idle time, the connection will terminate.

On-Demand is commonly chosen for an environment using an ethernet connection as a primary interface, while IP Fallback is used to bring up this dialup connection as a backup.

Persistent: Select this option when the link is intended as a primary network connection.

On-Demand: Select this option when the link is intended as a fallback network connection.

Use Default Route: Select *Yes* to use the peer as the default route. Select *Yes* when this link is intended as a primary network connection and *No* when this link is intended as a fallback network connection.

Enable Advance Setup: Select *Yes* to modify modem control, the modem speaker and enter modem initialization string. Select *No* to leave the advanced options as defaults.

Maximum Receive Idle Time (Required): Enter the number of seconds the connection may be allowed to remain "idle" or "unresponsive" (no data received) before closing the connection. If packets are leaving the interface, but no return packet is received for the specified time, then the connection is reset. This can be useful for detecting an unresponsive situation where the network is down, the modem is in an unknown state, or other low level error may have occurred.

Note: If the normal usage of the device regularly has packets leaving the unit with no expected response, then premature disconnections may result. Outgoing UDP packets with no expected

Modem: Select *Yes* to use the modem control lines CD (Carrier Detect) and DTR (Data Terminal Ready). If you are having difficulty using your external modem, try alternating this value and re-testing.

RTS/CTS: Select *Yes* to set hardware flow control using RTS and CTS signals. If you are having difficulty using your external modem, try alternating this value and retesting.

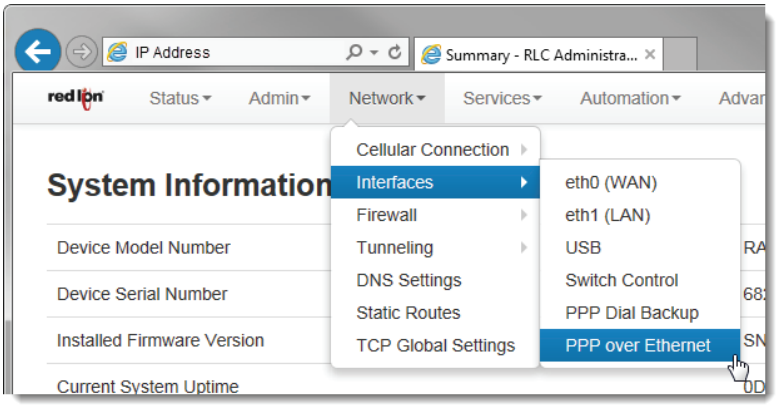
Modem Speaker On: Select *Yes* to turn on the modem speaker for testing and proof of concept phase to audibly verify connection attempts. Select *No* for silent production mode.

Enter Custom AT Command: Enter the modem initialization string. Please consult your modem AT Command documentation for unique initialization that may be required. Enter only a single initialization string.

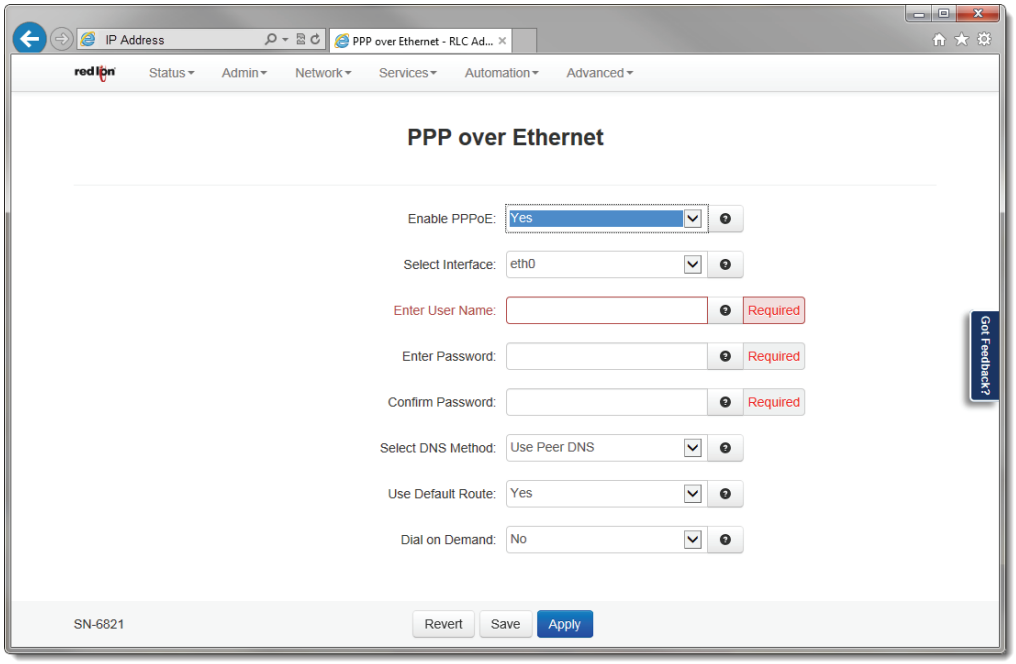
- Click on the "Save" button for changes to be saved without activating the interface, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.4.2.5 PPP over Ethernet

The PPP over Ethernet menu item is used to configure a connection by being able to connect a DSL or cable modem.



- Click on the PPP over Ethernet menu item and the following dialog window will appear:



Enable PPPoE: Select *Yes* to enable the PPP over Ethernet service on the specified interface when the Apply button is clicked. To disable the service, select *No* and click Apply.

Select Interface: Select the name of the Ethernet interface to which the PPP over Ethernet service should bind by choosing one of the options available in the provided drop-down list.

Enter User Name (Required): Enter the user name to be used with the PPPoE interface in the space provided. It is typically in the form *name@domain.com*.

Enter Password (Required): Enter the password to be used with the PPPoE interface in the space provided.

Confirm Password (Required): Re-input the password entered in the “Enter Password” field. This entry must match exactly the previously entered password.

Select DNS Method: Select the method by which DNS Server information should be obtained. The recommended setting for this field is "*Use Peer DNS*". Choices include:

Use Unit Default: Do not obtain DNS information from PPPoE Server. Use settings from ***Network->DNS Settings*** instead.

Use Peer DNS: DNS information should be obtained from the peer host once connected.

Use Custom DNS: DNS information is entered manually in the fields which will appear below.

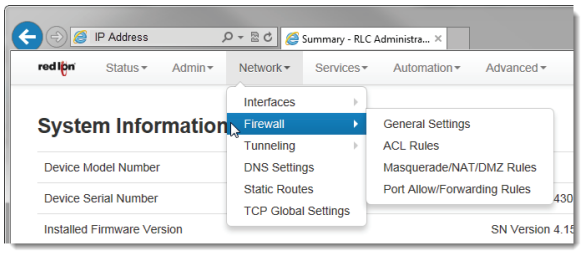
Use Default Route: Select Yes to use this interface as the default route.

Dial on Demand: Select Yes to enable this feature. The recommended setting for this field is No.

- Click on the "Save" button for changes to be saved without activating the interface, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.4.3 Firewall

The Firewall menu item allows you to configure every aspect of the firewall on the Red Lion router.

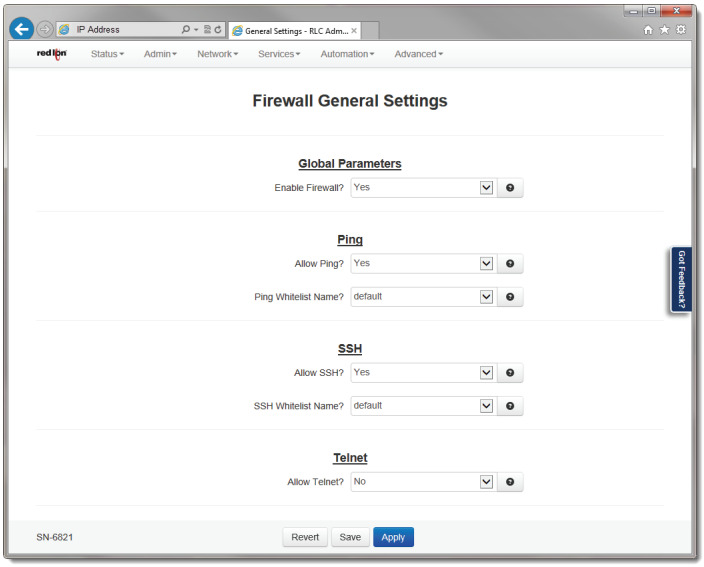


The Firewall menu is organized in four (4) sub-sections: General Settings, ACL Rules, Masquerade/NAT/DMZ Rules, Port Allow/Forwarding Rules.

3.4.3.1 General Settings (Firewall)

The General Settings menu is used to configure common access services to the Red Lion router and configure how the interfaces are interpreted.

- Click on the General Settings menu item and the following dialog window will appear:



Enable Firewall (Required): Specify whether to enable the firewall service on this device. The recommended setting for this field is *Yes*.

Note: Disabling the firewall will compromise security and routing functions of the unit.

Allow Ping: To allow ICMP echo responses (*Ping*) from external devices through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *Yes*.

To restrict access via a configured whitelist, select a whitelist name for the list of names available in the drop-down menu. **Note:** This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

Ping Whitelist Name: Select the desired whitelist from the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules>Subnet>Whitelist Rules*** screen.

Allow SSH: To allow external devices to connect to the SSH Server, via port 22, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *Yes*.

To restrict access via a configured Whitelist, click the check box marked **Use Whitelist** and then select a Whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the SSH server, it just allows it to be accessible via the firewall when it is enabled. The SSH Server may be enabled via the ***Services>SSH/TELNET Server*** screen.

If the SSH Server is configured to use a port other than 22, a rule specifically for the alternate port will need to be added via the Network>Firewall>Port Allow/Forwarding Rules>Service Access Rules screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

SSH Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the **Network>Firewall>ACL Rules> Subnet Whitelist Rules** screen.

Allow Telnet: To allow external devices to connect to the TELNET Server, via port 23, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *No*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the Telnet Server, it just allows it to be accessible via the firewall when it is enabled. The Telnet Server may be enabled via the Services>SSH/Telnet Server Screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

Telnet Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Allow Modbus: To allow external devices to connect to the MODBUS Server, via port 502, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *No*.

To restrict access via a configured whitelist, click the check box marked **Use Whitelist** and then select a whitelist name for the list of names available in the drop-down list box provided. Whitelist may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the MODBUS server, it just allows it to be accessible via the firewall when it is enabled. The MODBUS Server may be enabled via the A***utomation>ModBus>Forwarding*** screen.

Modbus Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Allow DNP3: To allow external devices to connect to the DNP3 Server, via port 20,000, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *No*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name for the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the DNP3 Server, it just allows it to be accessible via the firewall when it is enabled. Then DNP3 Server may be enabled via the ***Automation>DNP3>Physical Link Layer*** screen.

DNP3 Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Allow Web Interface Access: To allow external devices to connect to the Web Interface, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this feature is *Yes*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

Web UI Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Allow SNMP Agent Access: To allow external devices to connect to the SNMP Agent, via port 161, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this feature is *Yes*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the SNMP Agent, it just allows it to be accessible via the firewall when it is enabled. The SNMP Agent may be enabled via the ***Services>SNMP Agent*** screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

SNMP Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Allow IPSEC (Required): Specify whether to allow ESP data, as well as UDP port 500 to communicate with external devices through untrusted interfaces. The recommended setting for this field is *Yes*.

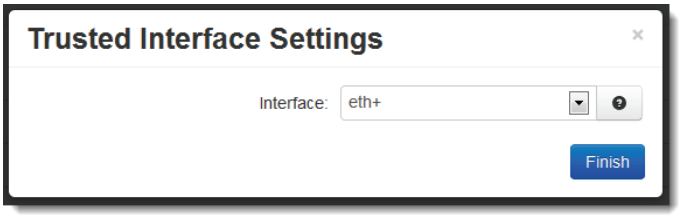
Note: This is necessary if you are planning to configure any IPSEC tunnels originating from this device.

Allow NAT-Traversal (Required): Specify whether to allow data on UDP port 4500 on untrusted interface. The recommended setting for this field is *Yes*.

Note: This is necessary if you are planning to run any IPSEC tunnels through our device. This would support a unit behind a trusted interface to make an IPSEC connection to a host beyond an untrusted interface.

Trusted Interfaces: Identifies the trusted (internal) interface. Traffic from this interface will be permitted outbound. Default is “WAN/eth0”.

- Click on the Add button for Trusted Interfaces and the following dialog window will appear:

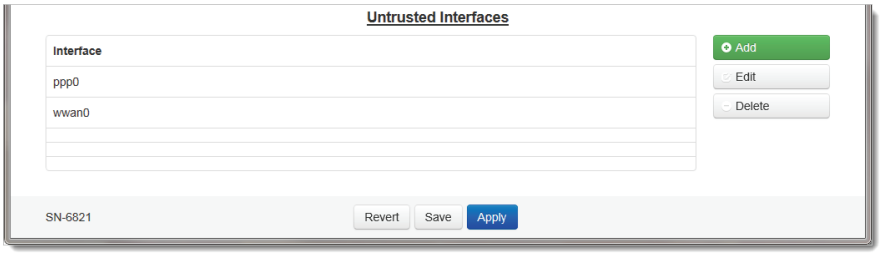


Interface: Choose an interface from the drop-down list provided. You may add as many interfaces as exist on the device. Each selection must be unique.

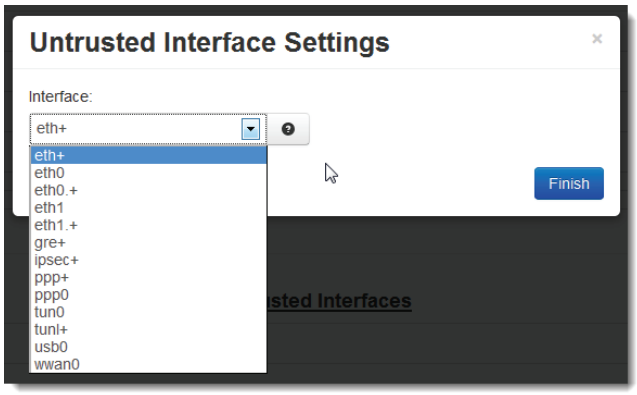
Trusted interfaces will not block traffic to/from devices connected to that interface. Filter Rules are the only rules that will control traffic on these interfaces.

- Click on the Finish button to populate the Trusted Interface screen.

Untrusted Interfaces: Identifies the Primary Untrusted (external) Interface and the following pop-up window will appear:



- Click on the Add button for Untrusted Interface and the following pop-up dialog window will appear:



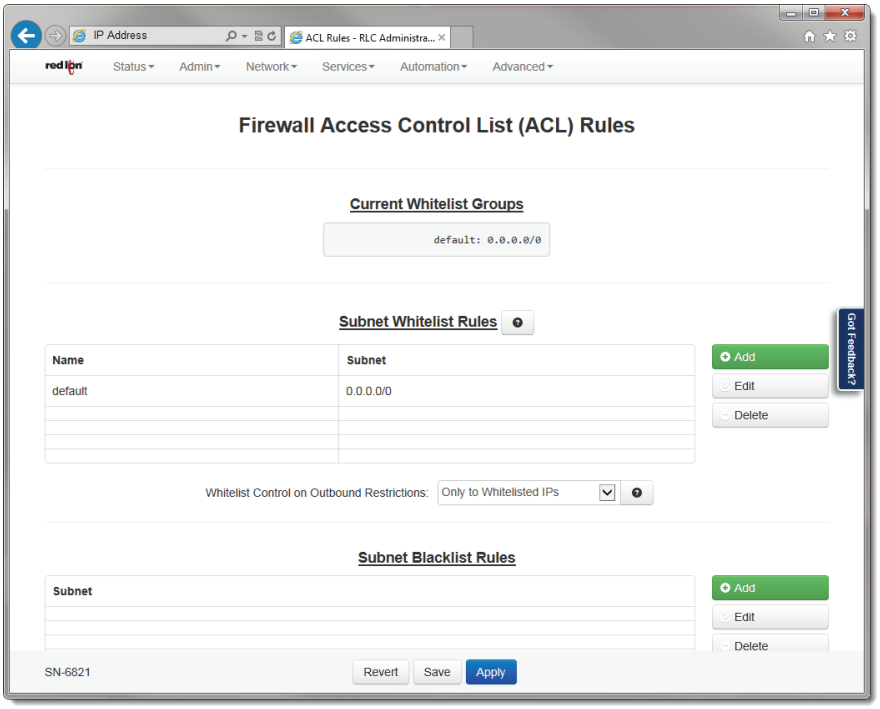
Interface: Choose an interface from the drop-down list provided. You may add any number of interfaces, up to as many exist on the device. Each selection must be unique.

Untrusted interfaces will block all incoming traffic from devices/networks connected to this interface. Exceptions must be defined in firewall rules to allow traffic (General Settings, Allow/Redirect, etc.)

- Click on the Finish button to populate the Untrusted Interface screen.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.3.2 ACL Rules - Firewall Access Control List Rules

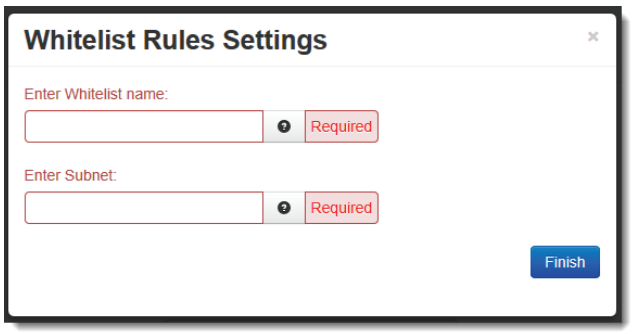
From the ACL Rules dialog window, Whitelist and Blacklist rules are defined. Whitelist Rules are used to define a single IP Address or an entire network that would be allowed to access the network behind the Red Lion router. Blacklist Rules are used to define a single IP Address or an entire network that are *NOT* allowed to access the network behind the router.



Current Whitelist Groups: This field is populated by the information entered in the Subnet Whitelist Rules Section.

Subnet Whitelist Rules: The Subnet Whitelist Rules are used to define a single IP Address or an entire network that you want to allow access into the network behind the Red Lion router.

- Click on the Add button and the following dialog window will appear:



Enter Whitelist Name (Required): Enter a name for the whitelist in the space provided. If the name of an existing whitelist is entered, then you are in effect adding another member to the list of subnets defined by that whitelist group.

After the Finish button is clicked, the entry will be added to the group in the (sorted) display area under the Current Whitelist Groups heading.

This whitelist name will become available for selection in the other Firewall Rules sections where a whitelist can be selected. ***Note:*** *The first whitelist entry, the 'default' entry may not be deleted or have its name changed, but its subnet value may be changed. Additional entries may be added, edited and deleted as needed.*

Enter Subnet (Required): Enter the network allowed to make connections to the above port(s), using IP/CIDR notation. To allow data from any source, enter 0.0.0.0/0. To specify a single host, use x.x.x.x/32, where x.x.x.x is the host's IP address.

- Click on the Finish button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Subnet Whitelist Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

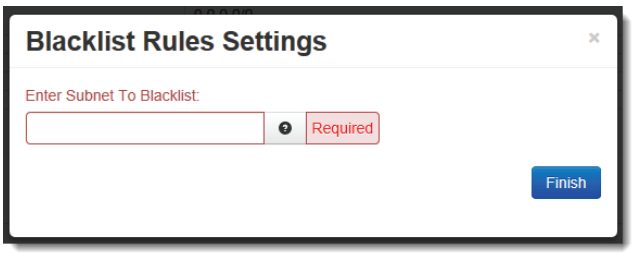
Whitelist Control on Outbound Restrictions: This setting controls whether or not the whitelist rules apply to packets originating from this device. There are two (2) choices:

Only to Whitelist IPs: Packets destined for subnets outside those allowed by the selected whitelist will be suppressed by the firewall.

No Restrictions: The device may send a packet to any subnet and the whitelist rules apply only to packets received.

Subnet Blacklist Rules: These rules are used to define a single IP Address or an entire network that are *NOT* allowed to access the network behind the Red Lion router.

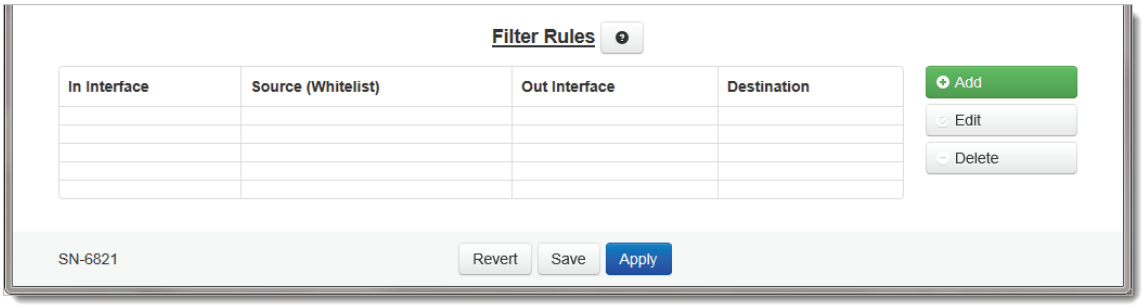
- Click on the Add button and the following window will appear:



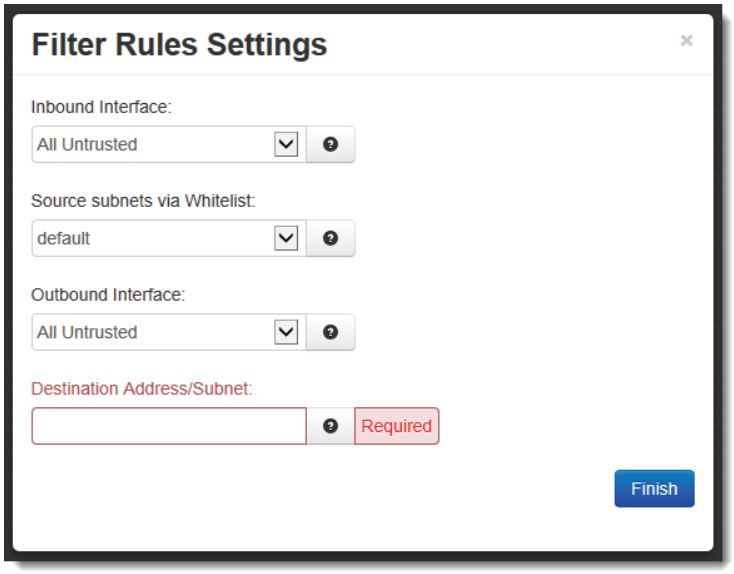
Enter Subnet To Blacklist (Required): Enter the network to be banned from making any incoming or outgoing connections, using IP/CIDR notation. To allow data from/to any source, enter 0.0.0.0/0. To specify a single host, use x.x.x.x/32, where x.x.x.x is the host's IP address. This will override any other sections rules (Allow/Redirect/DMZ/NAT/etc).

- Click on the Finish button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Subnet Blacklist Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

Filter Rules: Trusted interfaces are by default trusted, and do not have restrictions. Filter rules allow setting up specific paths that are allowed to communicate, applying even to trusted interfaces. This allows restricting traffic between internal, trusted (LAN) interfaces and can also restrict general traffic to untrusted (LAN) interfaces. ***Note:*** *Once any filter is configured for restricting traffic, ALL traffic is then dropped that does not match the filter(s) for specified interfaces. IPSEC traffic for VPN tunnels can also be filtered using these rules.*



- Click on the Add button and the following dialog window will appear:



Inbound Interface: Select an interface associated with the Source Address/Subnet from the drop-down menu.

Source Subnets via Whitelist: Select a whitelist name for the list of names available in the drop-down menu. Whitelists are defined in the ***Network>Firewall>ALC Rules>Subnet Whitelist Rules*** screen.

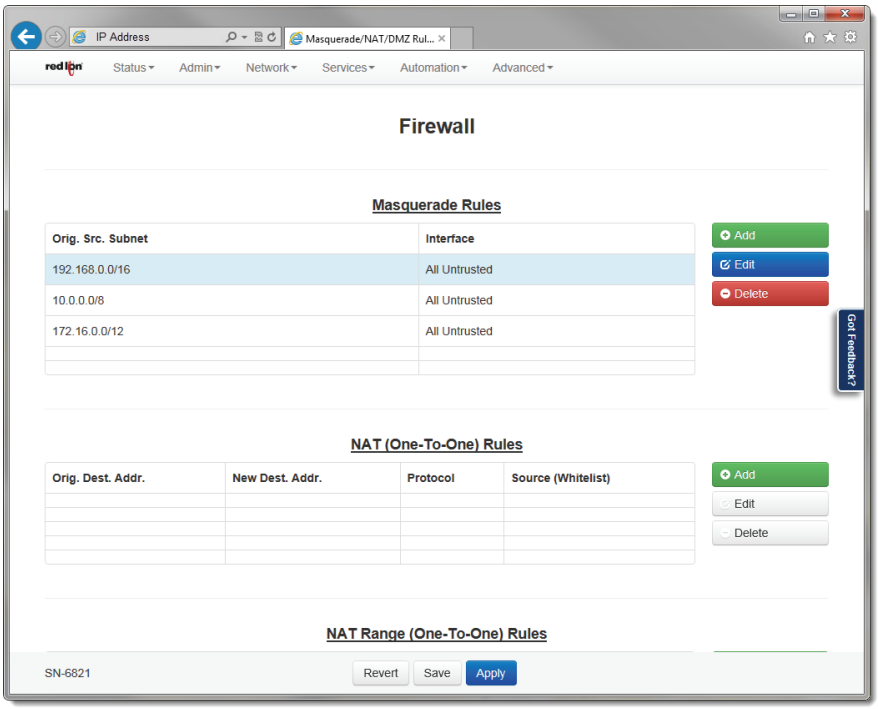
Outbound Interface: Select the interface associated with the Destination Address/Subnet.

Destination Address/Subnet (Required): Enter the network to which the firewall will allow access from the Outbound Interface.

- Click on the Finish button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Filter Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit butt
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

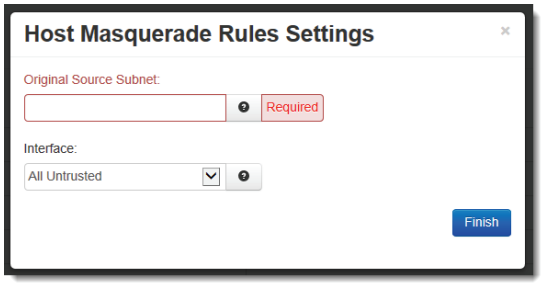
3.4.3.3 Masquerade/NAT/DMZ Rules

DMZ rules are used to configure rules to route through a Demilitarized Zone (DMZ), Masquerade rules are used to configure an interface to give all IP Addresses on a local network access to the internet, while NAT(Network Address Translation) rules provide access to the Internet through a single machine that translates the IP addresses.



Masquerade Rules: The MASQ rules enable access to the Internet through a single unit/interface that translates the IP addresses. The unit itself has one or more IP addresses, but all the IP’s behind the MASQ have ‘private’ Internet addresses.

- Click on the Add button and the following dialog window will appear:



Original Source Subnet (Required): Enter the subnet, using IP/CIDR notation that will be masqueraded out of a specific interface. All traffic that is sourced from this subnet and that is destined to go out the specified interface will be masqueraded with the source IP address of the interface specified.

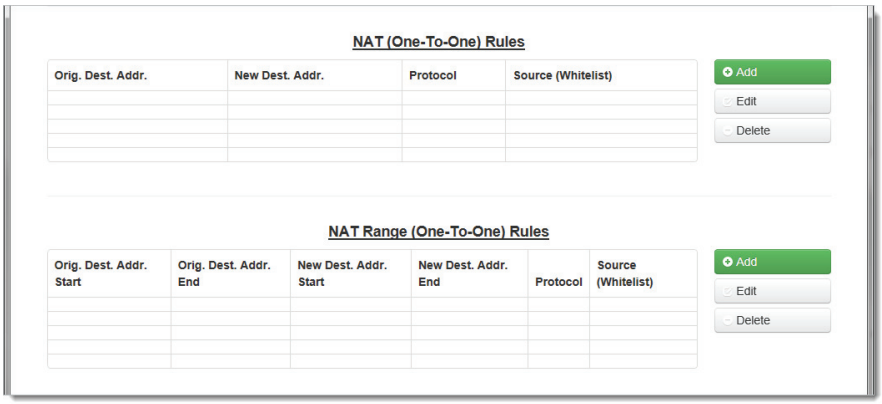
Interface: Select the desired interface through which you wish to masquerade source addresses from the drop-down menu.

- Click on the Finish button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the Masquerade Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

NAT (Network Address Translation) Rules: The NAT Rules enables access to the Internet through a single machine that translates the IP addresses. The NAT itself has one or more IP addresses, but all the machines behind the NAT have 'private' Internet addresses.

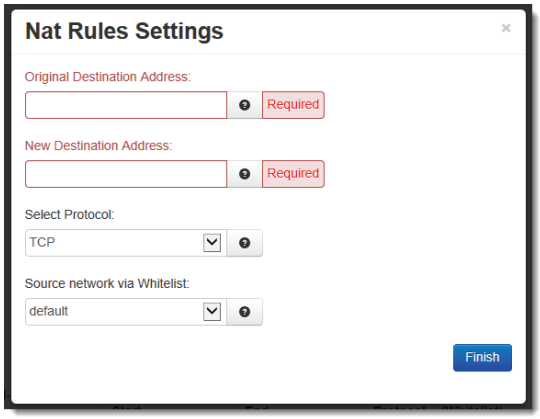
One-to-One NAT will perform a complete forwarding of app ports on the Original Destination IP to a new IP address entered in New Destination. Because the Original Destination need not be configured on this router, an interface is not required to setup.

One-to-One NAT Range will perform the same operation as a single One-to-One rule, but over a range of matched IP Addresses. The pool defined by the Original IP Start -> End (the first Original IP will always translate to the first New IP, the second to the second, etc). The number of entries in each pool must match.



NAT (One-to-One) rule:

- Click on the Add button and the following pop-up window will appear:



Original Destination Address (Required): This field holds the address being transformed by NAT, the IP seen by a remote host. This address may be owned by an interface on this device or an unowned/fake range with a corresponding route (static or default). One-to-one NAT will perform a complete forwarding of all ports on the Original Destination IP to a new IP address entered in New Destination. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

New Destination Address (Required): This field holds the real LAN IP of the destination device behind this router. One-to-one NA will perform a complete forwarding of all ports on the Original Destination IP to a new IP address entered in New Destination. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

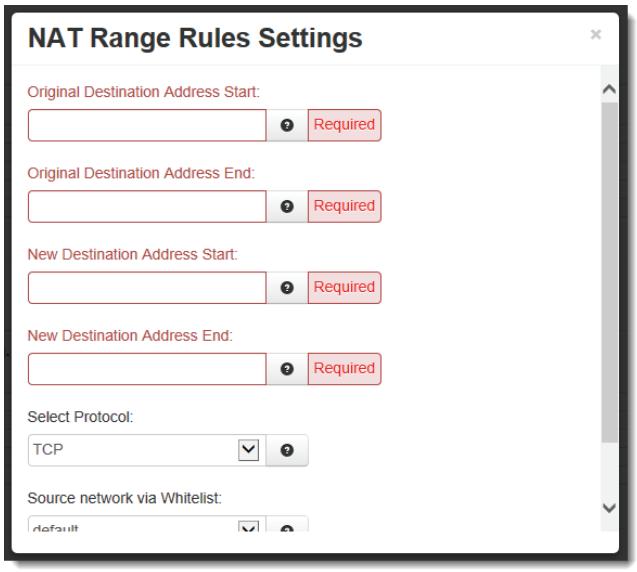
Select Protocol: Choose the protocol type for this port's data. Options are TCP, UDP, All.

Source network via Whitelist: Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

- Click on the Finish button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

NAT Range Rules:

- Click on the Add button and the following pop-up window will appear:



Original Destination Address Start (Required): This field holds the starting address range being transformed by NAT, the IP's seen by a remote host.

This address may be owned by an interface on this device, oran unowned/fake range with a corresponding route (static or default). One-to-one NAT Range will perform a complete forwarding of all ports on the starting Original Destination IP to a starting new IP address entered in the New Destination Address Start field. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

Original Destination Address End (Required): This field holds the ending address range being transformed by NAT, the IP's seen by a remote host.

This address may be owned by an interface on this device, or an unowned/fake range with a corresponding route (static or default). One-to-one NAT Range will perform a complete forwarding of all ports for the range of starting/ending Original Destination IP's to a range of starting/ending New Destination IP addresses entered in New Destination Address Start and New Destination Address End fields. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

New Destination Address Start (Required): This field is used to hold the starting range of real LAN IP of the destination device behind this router.

One-to-One NAT Range will perform the same operation as a single One-to-One Rule, but over a range of matched IP Addresses. The pool defined by the Original IP Start->End, will be matched to the pool defined by New IP Start-> End (the first Original IP will always translate to the first New IP, the second to the second, etc.). The number of entries in each pool must match. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

New Destination Address End (Required): This field is used to hold the ending range of real LAN IP of the destination device behind this router.

One-to-One NAT Range will perform the same operation as a single One-to-One rule, but over a range of matched IP Addresses. The pool defined by the Original IP Start->End, will be matched to the pool defined by New IP Start->End (the first Original IP will always translate to the first New IP, the second to the second, etc.). The number of entries in each pool must match. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

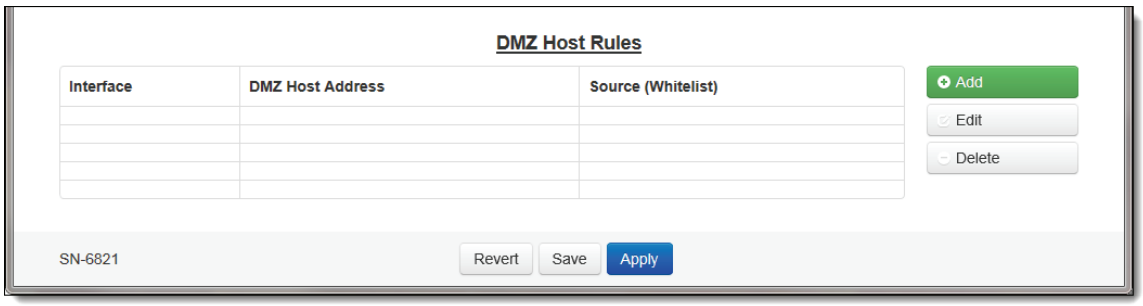
Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

Select Protocol: Choose the protocol type for this port's data. Options are TCP, UDP, All.

Source Network via Whitelist: Select a whitelist name for the list of names available in the drop-down list. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

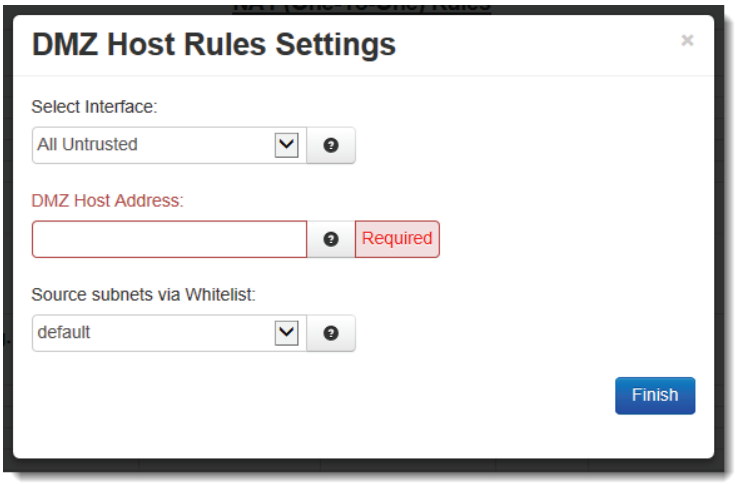
- Click on the Finish button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

DMZ Rules: DMZ rules are used to configure routes through a Demilitarized Zone (DMZ).



To add a DMZ host rule:

- Click on the Add button and the following dialog window will appear:



Select Interface: Click on the pull down-down menu to choose an interface that will be forwarded to a DMZ Host. All incoming packets (TCP/UDP/ICMP/etc) will be forwarded to the DMZ Host specified.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the DMZ Host.

DMZ Host Address (Required): Enter the IP address of the DMZ Host. This IP address will receive all packets destined for the interface specified. ***Note:*** *Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the DMZ Host.*

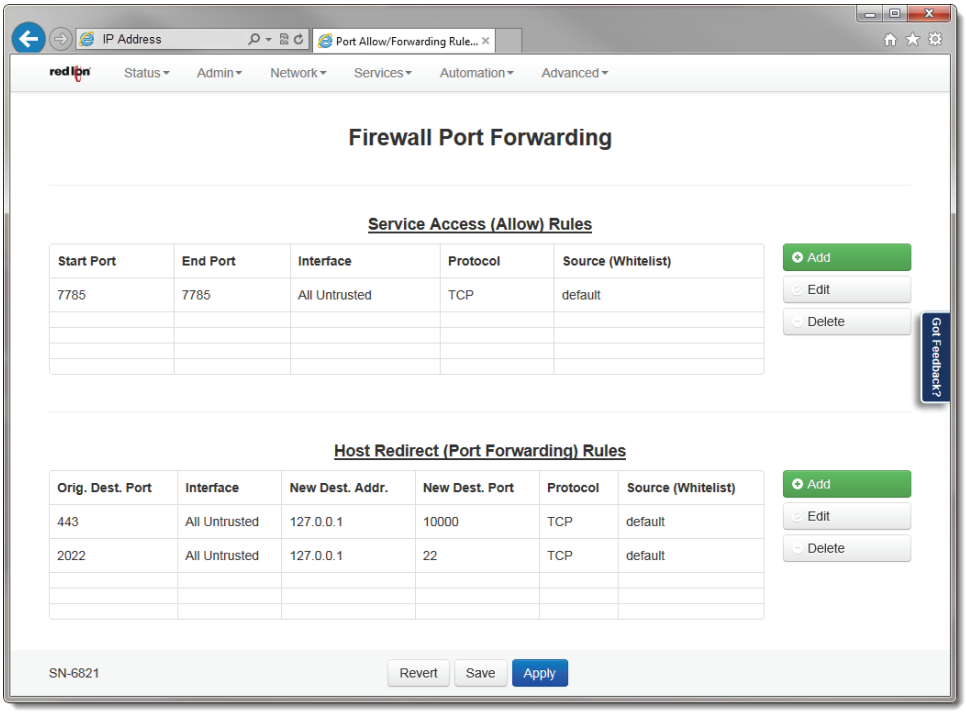
Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the DMZ Host.

Source subnets via Whitelist: Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

- Click on the Finish button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.3.4 Port Allow/Forwarding Rules

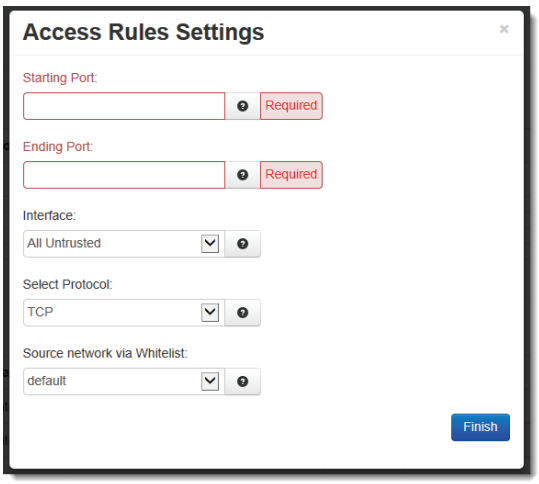
The Firewall Port Forwarding is used to configure routes from a small range of IP Addresses or all IP Addresses through one or more interfaces to a designated IP Address located behind the Red Lion router.



Service Access (Allow) Rules: The Service Access Rules option is used to define what ports, either as a single port or a range of ports, are authorized access through the firewall on the Red Lion router.

To add a new Service Access Rule:

- Click on the Add button and the following dialog window:



Starting Port (Required): Enter the starting TCP or UDP port number for this rule. ***Note:*** *If adding only one port, enter it here.*

Ending Port (Required): Enter the ending TCP or UDP port number for this rule. ***Note:*** *If adding only one port, please omit this entry.*

Interface: Select the interface on which this port will be opened. Incoming connections to this interface will be allowed into the device. ***Note:*** *For connections destined to a device beyond this unit, use Host Redirect, NAT or DMZ rules instead.*

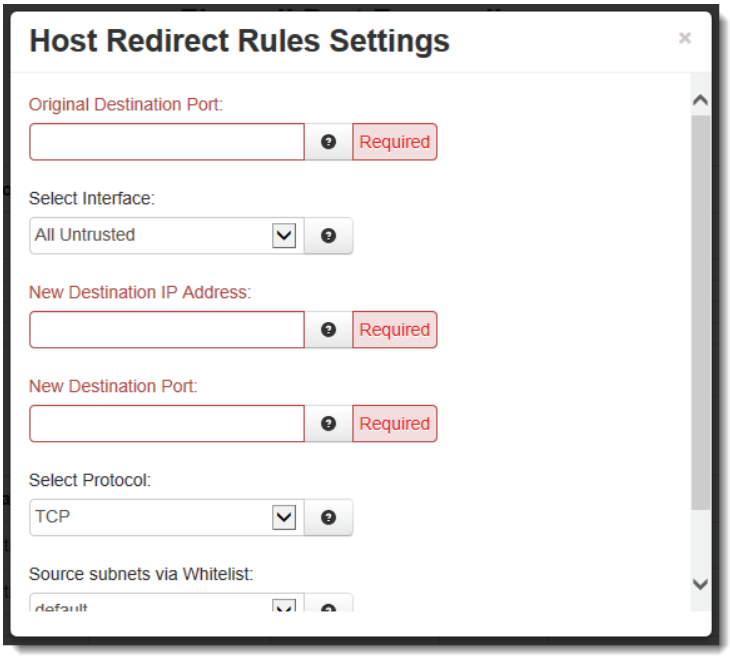
Select Protocol: Choose the protocol for the type of data you want to allow.

Source Network via Whitelist: Select a whitelist name from the list of names available in the drop-down list. Whitelists may be viewed/defined in the via the **Network/Firewall/ACL Rules** screen.

- Click on the Finish button. You will be returned to the Firewall Port Forwarding dialog window and the Service Access (Allow) Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

Host Redirect (Port Forwarding) Rules: The Host Redirect Rules option is used to configure port forwarding rules that permit ports on external, untrusted interfaces to be passed to ports on internal hosts on the same or different ports.

- Click on the Add button on the following dialog window will appear:



Original Destination Port (Required): Enter the port that an external device will try to connect to. This is the port that will be open on the specified interface.

Select Interface: Select the interface on which to open the specified port. Incoming connections will be allowed.

New Destination IP Address (Required): Enter the IP Address that the incoming connection will be redirected to. This can be an IP Address within or beyond this device.

New Destination Port (Required): Enter the port that the incoming connection will be redirected to. This may be the same number as the Original Destination Port.

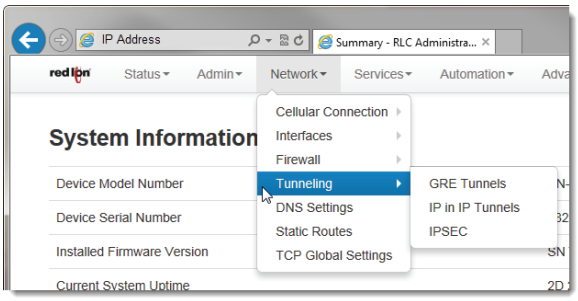
Select Protocol: Choose the protocol type for this port's data. Options are TCP and UDP.

Source Subnets via Whitelist: Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined in the via the **Network/Firewall/ACL Rules** screen.

- Click on the Finish button. You will be returned to the Firewall Port Forwarding dialog window and the Host Redirect (Port Forwarding) Rules table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the "Save" button for changes to be saved without activating the interface until you reboot the unit, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.4.4 Tunneling

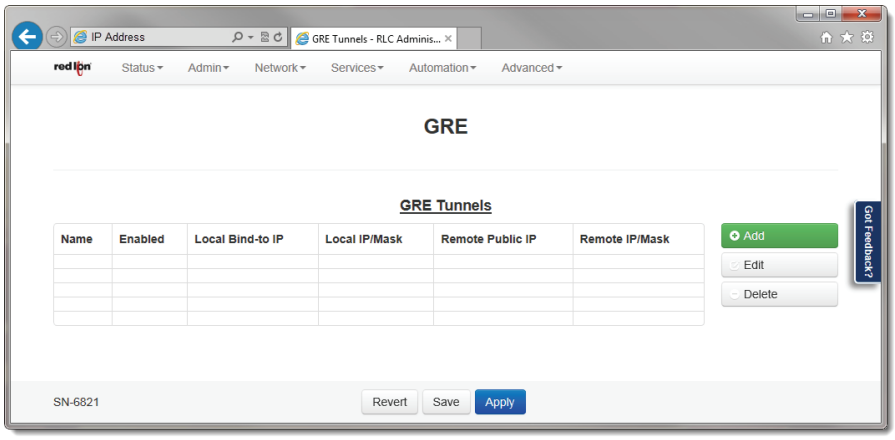
The Tunneling menu is divided into two (3) sub-sections: GRE Tunnels, IP in IP Tunnels and IPSEC.



3.4.4.1 GRE Tunnels (Generic Routing Encapsulation)

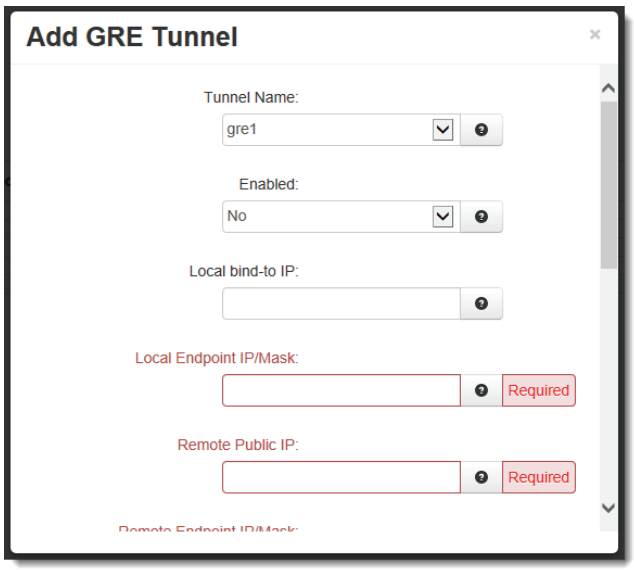
The GRE Tunnels menu item is used to configure a GRE Tunnel. GRE is a tunneling protocol that was originally developed by Cisco. It can do a few more things than IP-in-IP tunnelling. For example, you can also transport multicast traffic and IPv6 through a GRE tunnel.

- Click on the GRE Tunnels menu item and the following dialog window will appear:



To add a GRE Tunnel:

- Click on the Add button and the following window will appear:



Tunnel Name: Select the name of the GRE name by choosing one of the options available in the provided drop-down list.

Enabled: Select Yes to enable the tunnel.

Local bind-to IP: Set the local bind IP address for tunneled packets. This field is optional. **Note:** If supplied, the Local IP Address must be an address on another interface of this host. If not supplied, tunneled packets can be received from any interface.

Local Endpoint IP/Mask (Required): Set the local GRE IP Endpoint IP/mask.

Remote Public IP (Required): Set the Remote Public IP for this GRE connection.

Remote Endpoint IP/Mask (Required): Set the Remote GRE IP Endpoint IP/mask.

Inbound Key: Specify a key for use with keyed GRE. Key is either a number or an IP address. The Inbound Key is used for input only. This is an optional field.

Outbound Key: Specify a key for use with keyed GRE. Key is either a number or an IP address. The Outbound Key is used for output only. This is an optional field.

Time-to-Live (Required): Set a fixed Time-to-Live for tunneled packets. The recommended setting for this field is 64. Values over 64 may cause connection failures.

Use Multicast: Select Yes to enable Multicast for the tunnel.

Use ARP: Select Yes to enable ARP for the tunnel.

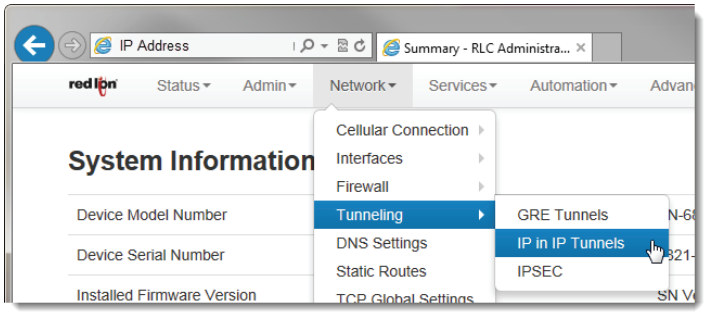
Start Tunnel at Boot: Select Yes to allow the interface to become active at system start.

- Click on the Finish button. You will be returned to the GRE Tunnels dialog window and the Configuration Table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

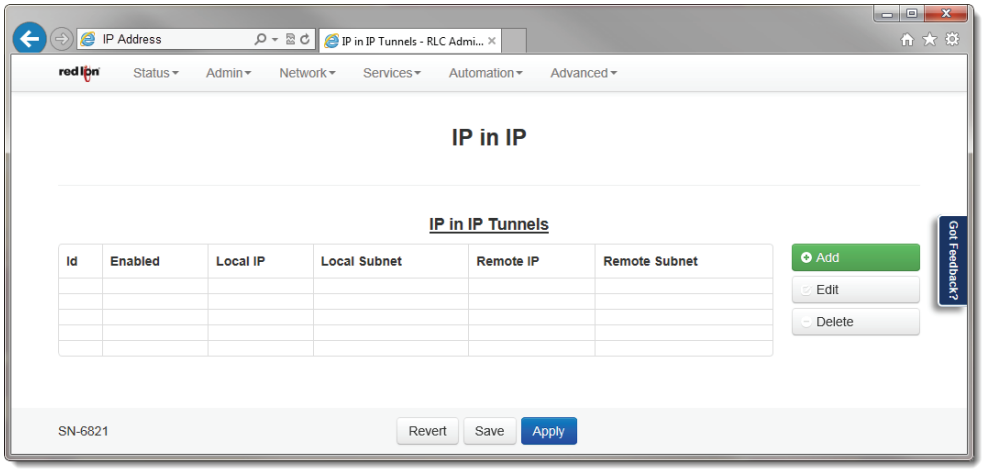
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.4.2 IP in IP Tunnels

The IP in IP Tunnels menu items is used to configure a simple IP Tunnel. IP in IP Tunnel essentially encapsulates an IP packet into another packet with the same protocol as the transport protocol.

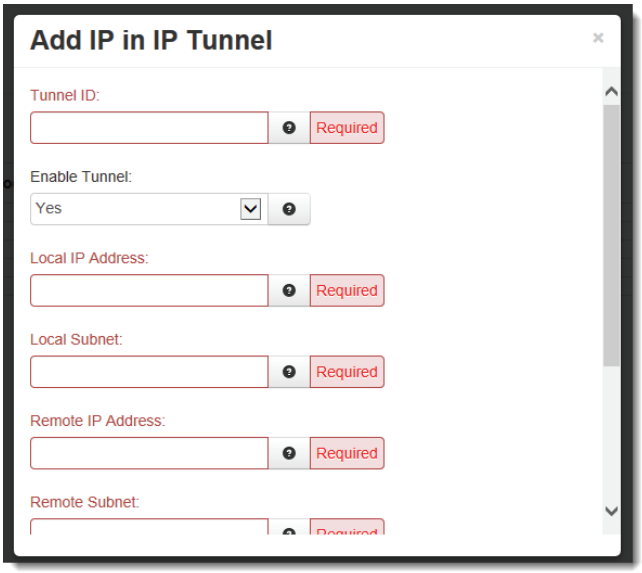


- Click on the IP in IP Tunnels menu item and the following window will appear:



To add an IP in IP Tunnel:

- Click on the Add button and the following window will appear:



Tunnel ID (Required): Enter a unique numerical identifier in this field. It will be used for naming the tunnel interface which will appear in the interface list as tunl1, tunl2, etc. depending on the IDs provided.

Enable Tunnel: Select Yes to enable the tunnel.

Local IP Address (Required): Set the fixed local address for tunneled packets. Note: If supplied, the Local IP Address must be an address on another interface of this host. If not supplied, tunneled packets can be received from any interface.

Local Subnet (Required): Set the local, private IPP network/mask.

Remote IP Address (Required): Set the IP Address of the remote endpoint for this tunnel.

Remote Subnet (Required): Set the remote, private IP network/mask.

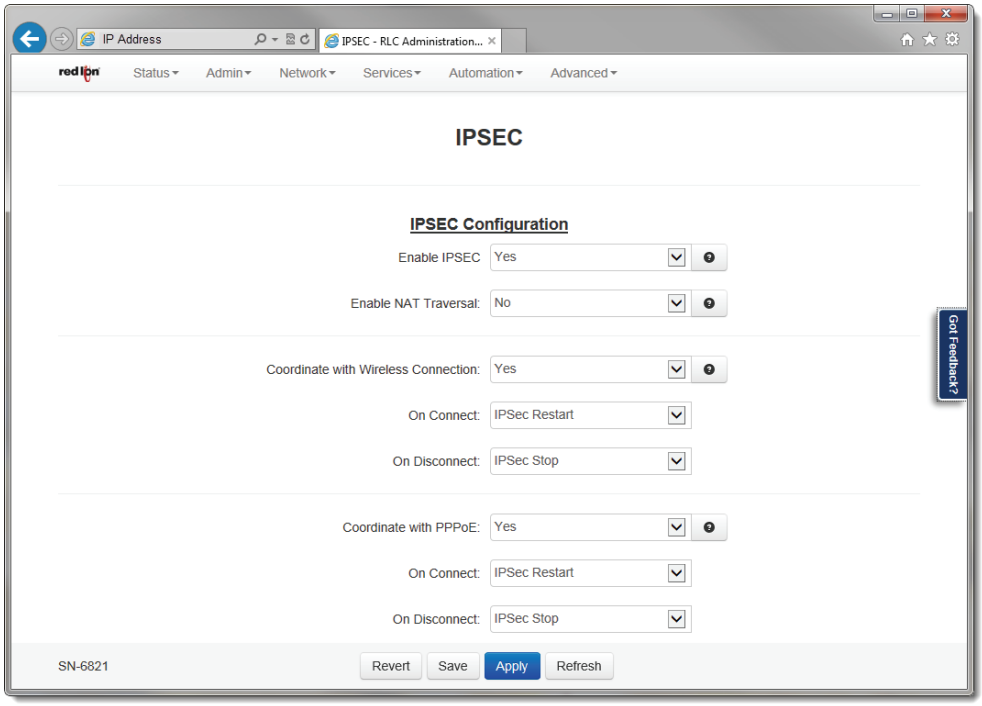
Time-To-Live (Required): Set a fixed Time-To-Live for tunneled packets. Note: Values over 64 cause connection failures.

Start Tunnel at boot: Select Yes to allow the interface to become active at system start.

- Click on the Finish button. You will be returned to the IP in IP dialog window and the IP in IP Tunnels Table will now be populated with the recently entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.4.3 IPSEC

The IPSEC dialog window is split into two sections. The top section pertains to the IPSEC configuration and the bottom portion is where IPSEC tunnels are created and edited.



IPSEC Configuration

Enable IPSEC: Specify whether you want to enable the IPSEC service. If you select No, all tunnels will be disabled.

Enable NAT Traversal: Specify whether all tunnels will use NAT Traversal.

Coordinate with Wireless Connection: You may select specific actions to be performed either upon PPP connect, PPP disconnect or both. The available actions include:

Do Nothing: Perform no action

Restart: IPSEC is restarted

Stop: IPSEC is stopped

With these combinations, the connection management may be fine-tuned so that the tunnel(s) may be able to restart faster, rather than having to rely on Dead Peer detection or other time out mechanisms alone.

Coordinate with PPPoE: You may select specific actions to be performed either upon PPP connect, PPP disconnect or both. The available actions include:

Do Nothing: Perform no action

Restart: IPSEC is restarted

Stop: IPSEC is stopped

With these combinations, the connection management may be fine tuned so that the tunnel(s) may be able to restart faster rather than having to rely on Dead Peer detection or other time out mechanisms alone.

Coordinate with Dial-up PPP: You may select specific actions to be performed either upon PPP connect, PPP disconnect or both.

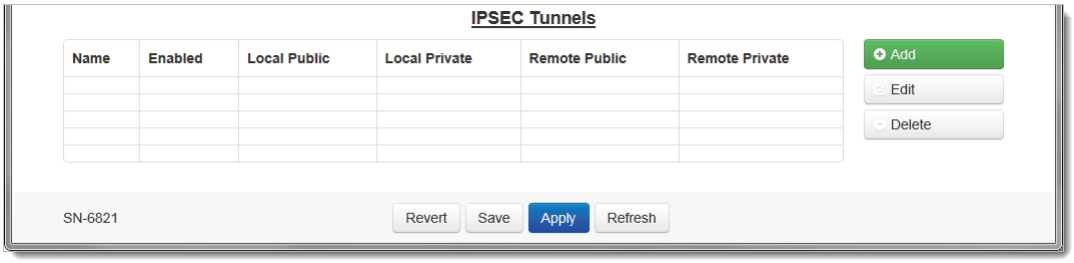
Do Nothing: Perform no action

Restart: IPSEC is restarted

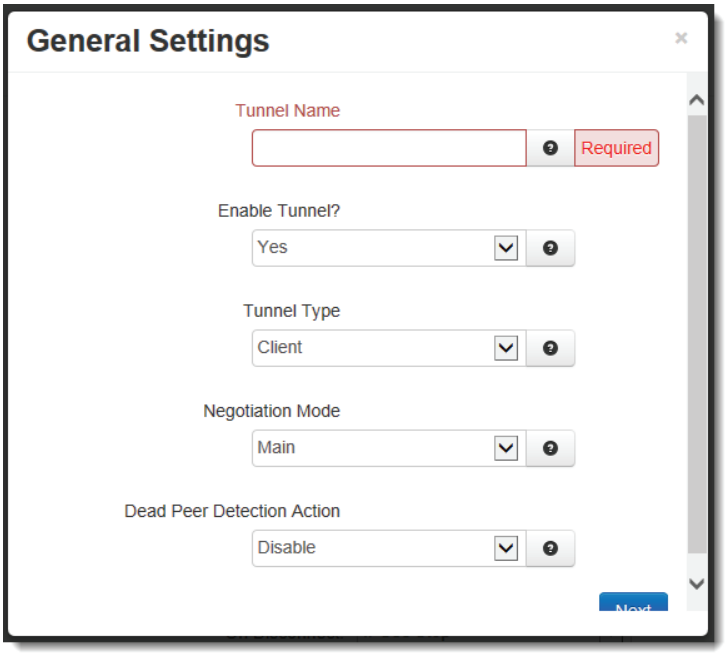
Stop: IPSEC is stopped

With these combinations, the connection management may be fine tuned so that the tunnel(s) may be able to restart faster rather than having to rely on Dead Peer detection or other time out mechanisms alone.

IPSEC Tunnels



- Click on the Add button and the following **General Settings** dialog window will appear:



Tunnel Name (Required): Enter some descriptive text in this field as an aid identifying it. The value must not contain spaces.

Enable Tunnel: Specify whether this tunnel should connect to its remote peer now and after any reboot.

Tunnel Type: Controls the initial mode of the tunnel at startup. The options given to IPsec will be:

Client: auto=start

Server: auto=add

Dynamic: auto=route

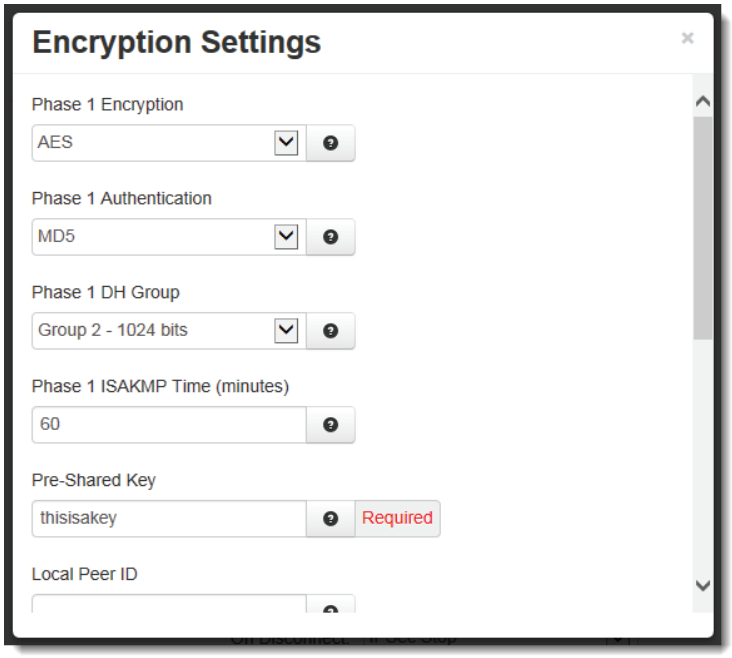
For more information, please consult an IPsec user guide on aspects of these specific modes.

Negotiation Mode: As a default, this field is set to Main mode ISAKMP Negotiation. When using dynamic, or DHCP issued IP addresses (for example with cellular cards), some remote devices may require the use of Aggressive Mode ISAKMP Negotiation. Should you encounter this situation, you can perform aggressive mode ISAKMP negotiation by changing this parameter from “Main” to “Aggressive ISAKMP”. To use Aggressive ISAKMP Negotiations, select Yes from the list provided or No to prevent it’s use.

Dead Peer Detection Action: This feature can help detect when a remote end-point is no longer communicating properly. Once an error is detected, the “hold” state will only renegotiate the tunnel after new traffic destined for the tunnel is detected. The “restart” state will attempt to immediately re-establish the connection to the concentrator. For this reason, “restart” may use more bandwidth and may not be the ideal choice for a limited data plan. However, if a host at the central site needs to initiate connections down to a local device through the tunnel, “restart” may be necessary so that the tunnel is always up and waiting for new data from the concentrator.

Use Perfect Forward Secrecy: Specifies whether or not the tunnel will use Perfect Forward Secrecy when negotiation cryptography parameters with the remote device. **Note:** This parameter must be set the same on the devices on both sides of the tunnel in order for a Security Association (SA) to be established. This is one of the first things that should be checked when tunnel negotiation difficulties are encountered.

- Click on the NEXT button and the following **Encryption Settings** dialog window will appear:



Phase 1 Encryption: Select the type of encryption needed for phase 1 (IKE).

Phase 1 Authentication: Select the type of authentication needed for phase 1 (IKE).

Phase 1 DH Group: Select the DH Group needed for phase 1 (IKE) by choosing one of the values from the drop-down list provided. This option selects the encryption level of the Diffie-Hellman keys and these are Group 1 (768 bits), Group 2 (1024 bits), Group 5 (1536 bits) or Group 14 (2048 bits). Longer keys imply better security but at a cost of longer negotiation/set-up time during the initial connection establishment. These settings must match on both ends of the connection. A value of *None* means that no DH Group will be selected for this end of the tunnel and it will adopt the settings of its peer during connection initiation.

Phase 1 ISAKMP Time (minutes): Select how long, in minutes, the keying channel of a connection (ISAKMP SA) should last before being renegotiated.

Pre-Shared Key (Required): Specify the key to be exchanged for encryption negotiation during phase (IKE). Key must not contain a double-quote character. **Note:** The Pre-Shared Key must match on both ends of the tunnel in order to work.

Local Peer ID: Specify how the left participant should be identified for authentication. Can be an IP address of a fully qualified domain name preceded by @ (which is used as a literal string and not resolved).

Remote Peer ID: Specify how the right participant should be identified for authentication. Can be an IP address of a fully qualified domain name preceded by @ (which is used as a literal string and not resolved).

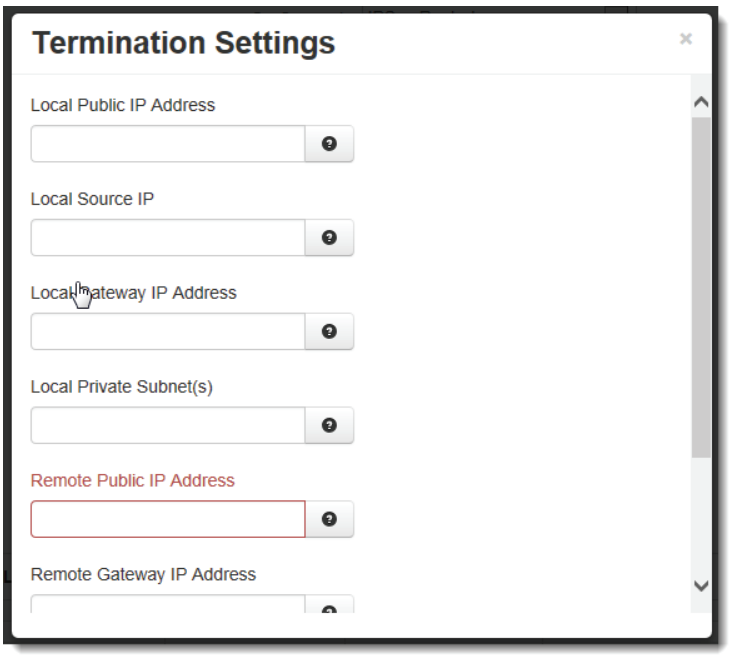
Phase 2 Auth Type: Defines whether authentication should be done as part of ESP encryption, or separately using the AH protocol.

Phase 2 Encryption: Select the ESP encryption algorithm to be used for the connection.

Phase 2 Authentication: Select the ESP authentication algorithm to be used for the connection.

Phase 2 ISAKMP Time (minutes): Select how long, in minutes, a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiration.

- Click on the NEXT button and the following Termination Settings dialog window will appear:



Local Public IP Address: This parameter typically only needs to be specified when the Red Lion router is configured to use more than one external, untrusted interface. Specify the IP Address of the left participant's public network interface.

For example, if the Red Lion router has an external cellular interface (ppp0) and an external Ethernet interface that is connected to a cable or DLS modem, and you need to bind the tunnel's crypto endpoint to the Ethernet interface, you would specify the IP address of the appropriate Ethernet interface here.

Note: *If this value is omitted, it will be filled in automatically with the local address of the default route interface (as determined at IPSEC startup time).*

Local Source IP: Specify the Local IP Address to source when transmitting. The IP Address for this host to use when transmitting a packet to the other side of this link. Relevant only locally, the other end need not agree. This option is used to make the gateway itself use its internal IP, which is part of the left subnet or right. Otherwise, it will use its nearest IP Address, which is its public IP Address.

This option is primarily used when defining subnet-subnet connections, so that the gateways can talk to each other and the subnet at the other, without the need to build additional host-subnet, subnet-host and host-host tunnels.

Local Gateway IP Address: Specify the next-hop gateway, IP address for the left participant's connection to the public network. **Note:** If no value is provided, the tunnel will use the right participant as its next hop.

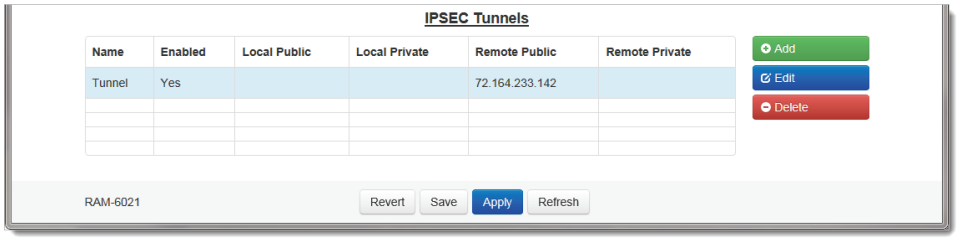
Local Private Subnet(s): Specify the private subnet(s) behind the left participant, expressed in CIDR format (xxx.xxx.xxx.xxx/nn) as network/netmask. More than one subnet can be specified by using a semi-colon to separate each entry.

Remote Public IP Address: Specify the IP address of Host name of the right participant's public-network interface. This field is required if Client is selected as Tunnel Type. If "Server" or "Dynamic" is selected as Tunnel Type, and this field is blank, then the value of **%any** will be used in the configuration file.

Remote Gateway IP Address: Specify the next hop gateway IP Address for the right participant's connection to the public network. **Note:** If no value is provided., the tunnel will use the left participant as it's next hop.

Remote Private Subnet(s): Specify the private subnet(s) behind the right participant, expressed in CIDR format (xx.xxx.xxx.xxx/nn) as network/netmask. More than one subnet can be specified by using a semi-colon to separate each entry.

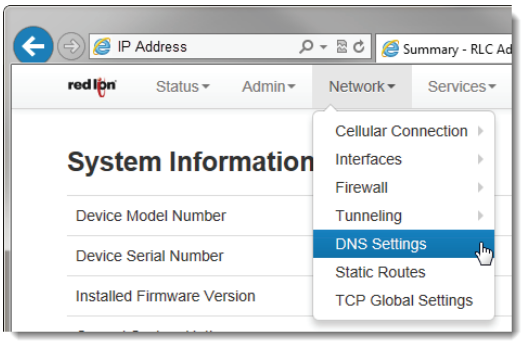
- Click on the Finish button. You will be returned to the IPSEC dialog window and the IPSEC Tunnels table will now be populated with the recently entered data.



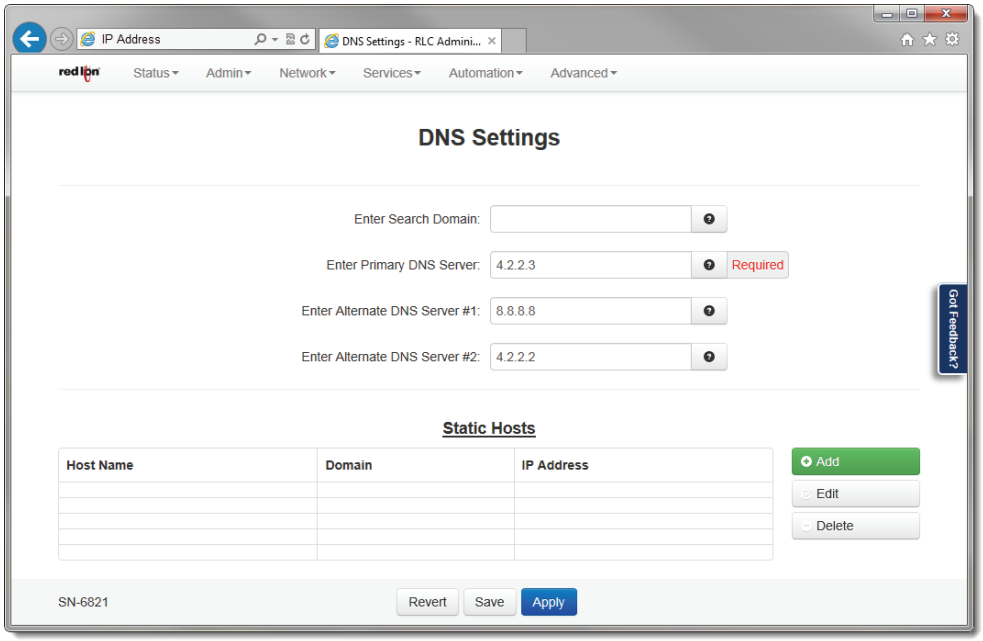
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the "Save" button for changes to be saved without activating the interface until you reboot the unit, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.4.5 DNS Settings

The Domain Name Server (DNS) Settings dialog window is split into two sections. The top section pertains to the DNS settings and the bottom section is where static hosts are added and edited.



- Click on the DNS Settings menu item and the following dialog window will appear:



Enter Search Domain: Enter the local domain name(s) to be searched, separated by spaces. These domains are used as the default local domains when performing DNS queries. **Example:** local.net domain.com

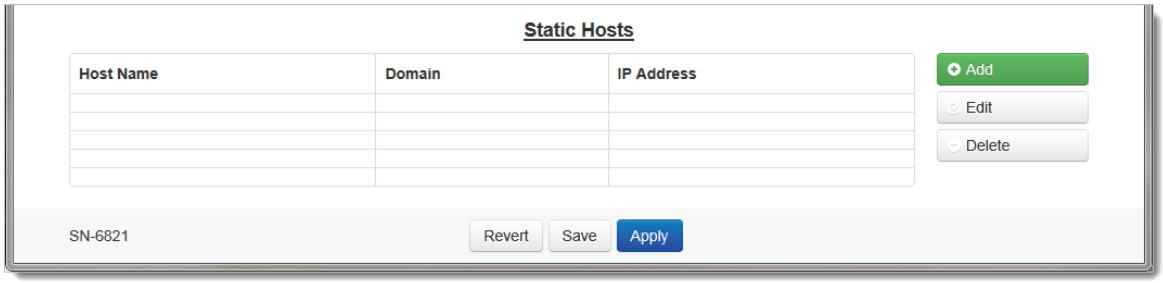
Enter Primary DNS Server (Required): *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of the Primary DNS Server you want to use. **Note:** This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

Enter Alternate DNS Server #1: *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of a Backup DNS Server you want to use, if the Primary DNS Server is unable to perform a DNS lookup. **Note:** This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

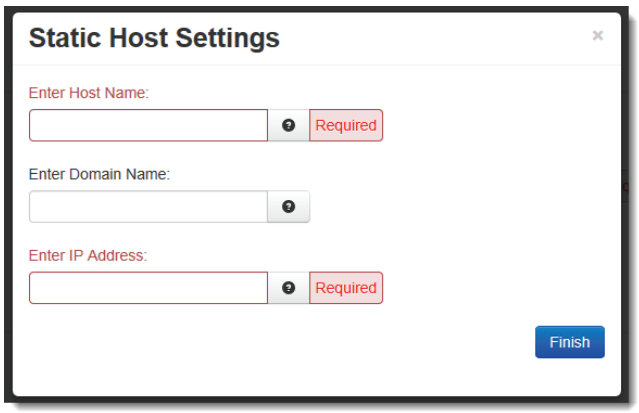
Enter Alternate DNS Server #2: *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of a Backup DNS Server you want to use, if the Primary DNS Server is unable to perform a DNS lookup. **Note:** This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

Static Hosts

Static Host entries may be added for local hosts, allowing the Red Lion router to resolve local host names to IP addresses.



- Click on the Add button on the following dialog window will appear:



Enter Host Name (Required): Enter the desired Host Name.

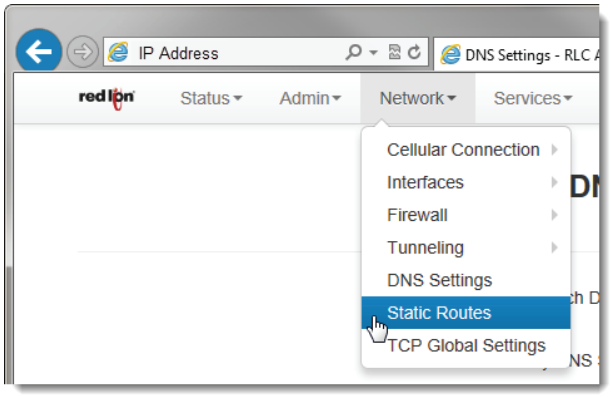
Enter Domain Name: Enter the desired Domain Name.

Enter IP Address (Required): Enter the host IP Address.

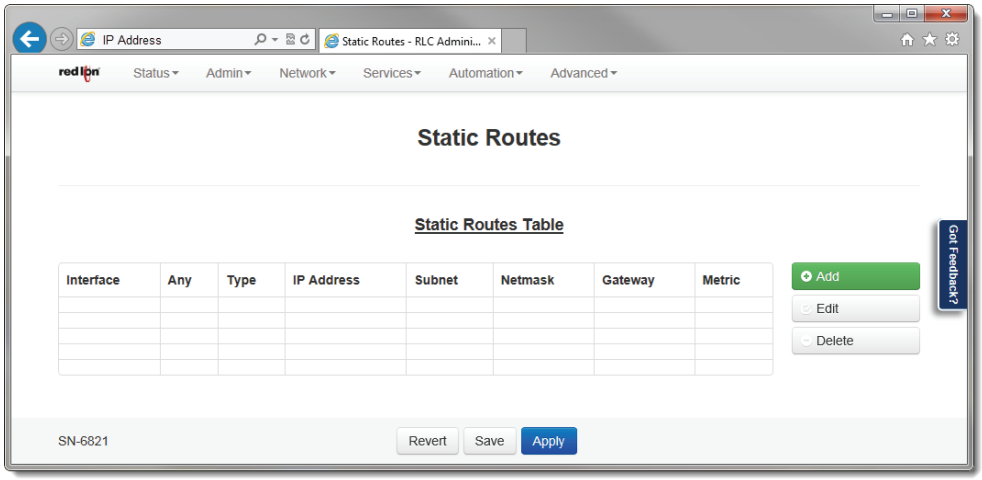
- Click on the Finish button. You will return to the DNS Settings dialog window and the Static Hosts table will now be populated with the recently entered data.
- To delete an existing host, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.6 Static Routes

The Static Routes menu allows you to configure a route to a network through an interface manually.

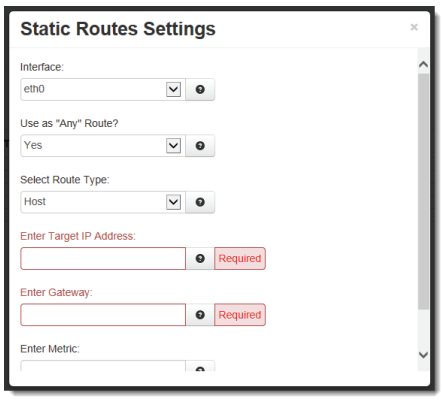


- Click on the Static Routes menu item and the following dialog window will appear:



To add a Static Route on the Red Lion router:

- Click on the Add button and the dialog window below will appear:



Interface: Select the interface to which the route should be applied by selecting one of the available options from the drop-down list. The available interfaces varies depending on the particular model of device, as well as the current configuration, and may include those created as aliases, VPN tunnels.

Use as "Any" Route?: Select whether or not this route should be used as an "any" route by selecting Yes or No from the provided drop-down list.

When set to **Yes**, the route will take effect when a network change event (up/down) occurs on any interface. For example, if the configured interface is set to eth0, and the ppp0 interface becomes active, then the route will be reapplied to eth0.

When set to **No**, the route will take effect only when a network change occurs on the configured interface. For example, if the configured interface is eth1, then the route will be assigned only when eth1 has a network change to an active state.

Select Route Type: Select the type of route to be created by choosing one of the available options from the provided drop-down list. The choices are Host or Network.

Select **Host** to create a route to a specific device. This will require setting the T**arget IP Address** and **Gateway** parameters.

Select **Network** to create a route to a remote network. This will require setting the **Network IP Address**, **Netmask** and **Gateway** parameters.

Enter Target IP Address (Required): Enter the IP Address of the destination host to which the route should be created.

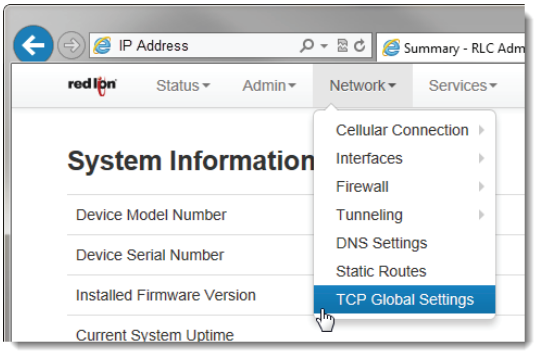
Enter Gateway (Required): Enter the IP Address of the gateway for the specified host or network. A gateway is a device (typically a router) used to gain access to another network.

For example, if a device is attached to a LAN whose a network address is 192.168.1.0 with a netmask of 255.255.255.0, than it can communicate directly with any other device on that network with a range of addresses of 192.168.1.1 through 192.168.1.254 (with 192.168.1.255 reserved for a broadcast). An address outside of that range is on a different network which would need to be accessed indirectly through a router and that router would be the gateway to the network on which the remote target device resides. In order to communicate with it, it would mean sending and receiving via the gateway device. The address must be one within the valid range for the network on which the designated interface resides.

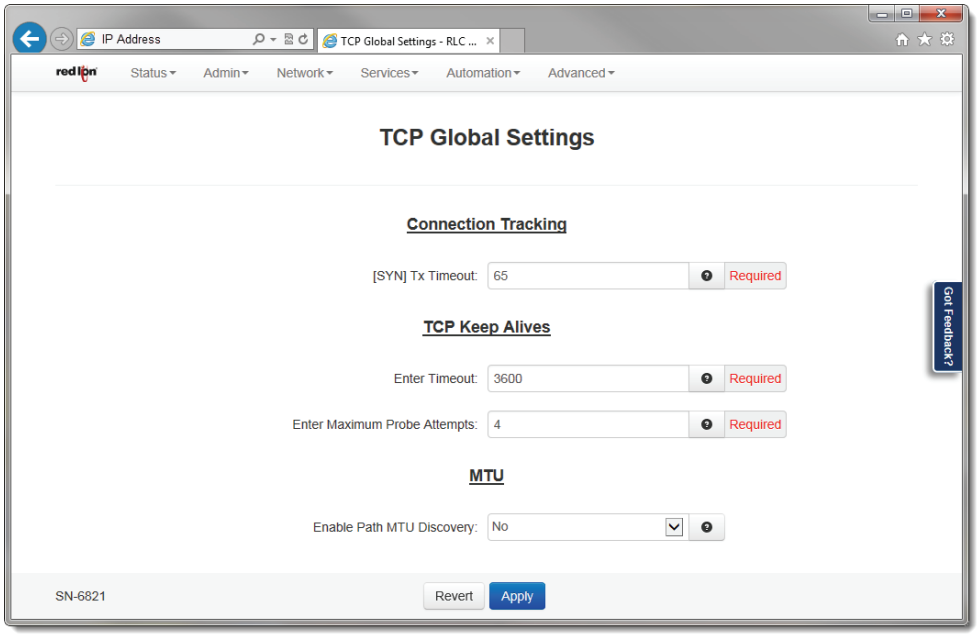
Enter Metric: Enter a value for the route metric in this field. Recommended value is 0.

- Click on the Finish button. You will return to the Static Routes dialog window and the Static Routes table will now be populated with the recently entered data.
- To delete a static route, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.4.7 TCP Global Settings



- Click on the TCP Global Settings menu item the following dialog window will appear:



[SYN] Tx Timeout (Required): Specifies the timeout value, in seconds, for SYN packets for connection tracking. 65 is generally recommended default, which differs from the system default of 120. The recommended default for IP ATMs is 30-120.

Enter Timeout (Required): Specifies the amount of time, in seconds, that a TCP connection can remain in an idle state before sending Keep-Alive Probes to verify that the remote end of the socket is still available. The recommended setting for this field is 10-30 for Ethernet connections where data usage is not an issue.

10 - 30 for Ethernet connections where data usage is not an issue.

60 - 300 for cellular connections where total data usage must be considered.

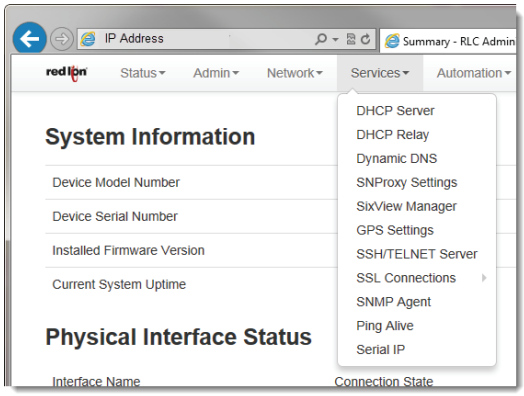
Enter Maximum Probe Attempts (Required): Specifies the acceptable number of failed probes that will be sent to the remote end of a TCP socket before determining the connection to be failed and disconnecting. The recommended values are 3-6.

Enable Path MTU Discovery: Enable/Disable Path MTU Discovery. This might be useful if a private cellular network is restricting MTU sizes along the network path and causing packet drops. The recommended value for this field is No (off).

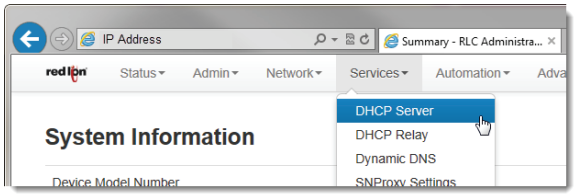
- Click on the Apply button to save the newly entered values. To revert to the previous defaults, click on the “Revert” button.

3.5 Services Tab

The Services Tab is where you can configure the various service offerings of the Red Lion router. These services include DHCP Server, DHCP Relay, Dynamic DNS, SNProxy Settings, SixView Manager, GPS Settings, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive and Serial IP.

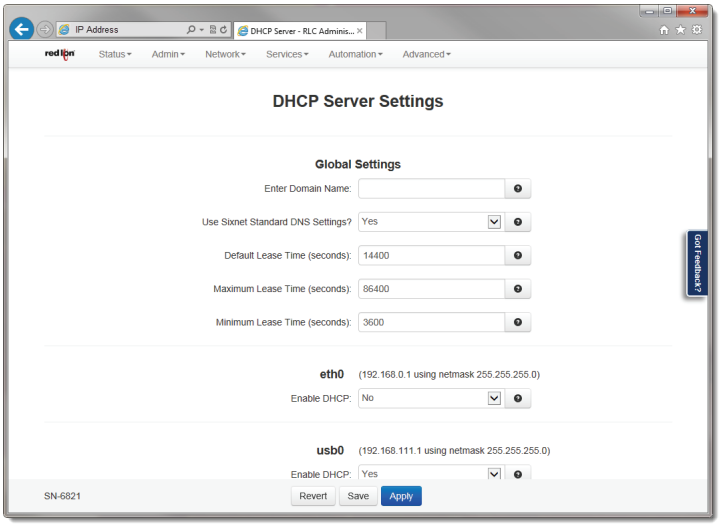


3.5.1 DHCP Server



Used to configure one of the internal Ethernet interfaces to be a DHCP server and hand out IP Addresses to systems connected to the Red Lion router.

- Click on the DHCP Server menu item and the following dialog window will appear:



Global Settings:

Enter Domain Name: Enter the domain name that will be passed to DHCP Clients.

Use Sixnet Standard DNS Settings:

- Choosing “Yes” will automatically use the DNS Servers obtained by this unit’s internet connection and/or entries specified in Networking→DNS Settings. This is the preferred method of operation.
- Choosing “No” will allow you to issue custom DNS servers to connected DHCP Clients. This will not affect any DNS Servers used by this unit for local domain resolution.

Default Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server will allow clients to maintain their leases. Default value is “**14400**” (4 hours).

Maximum Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server will allow clients to maintain their leases. Default “**86400**”(24 hours).

Minimum Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server will allow clients to maintain their leases. Default “**3600**”(1 hour).

eth0:

Enable DHCP: Specify whether you want to enable a DHCP Server for the interface. **Note:** If the interface is not enabled, or has been set to obtain its addressing parameters via DHCP, this option will be forced to “No”, and disabled until the interface is both enabled and set to use a static IP address.

Enable Default Gateway: Provide Default Gateway IP Address to DHCP Client. Select No if you wish to only gain access to this device’s web interface and have another connection from your PC out to the internet. Select Yes if you wish to gain access to the internet through this device.

Starting Address (Required): Enter the Starting IP Address of a range you want the DHCP Serer to provide for clients.

Recommended Setting: An address valid for the subnet for which the interface is configured. Care should be used to endure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Ending Address (Required): Enter the Ending IP Address of a range you want the DHCP Server to provide for clients.

Recommended Setting: An address valid for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

usb0:

Enable DHCP: Specify whether you want to enable a DHCP Server for the interface. **Note:** If the interface is not enabled, or has been set to *obtain* its addressing parameters via DHCP, this option will be forced to “NO”, and disabled until the interface is both enabled and set to use a static IP Address.

Enable Default Gateway: Provide Default Gateway IP Address to DHCP Client. Select NO if you wish to only gain access to this device’s web interface and have another connection from your PC out to the internet. Select YES if you wish to gain access to the internet through this device.

Starting Address (Required Field): Enter the Starting IP Address of a range you want the DHCP Server to provide for clients.

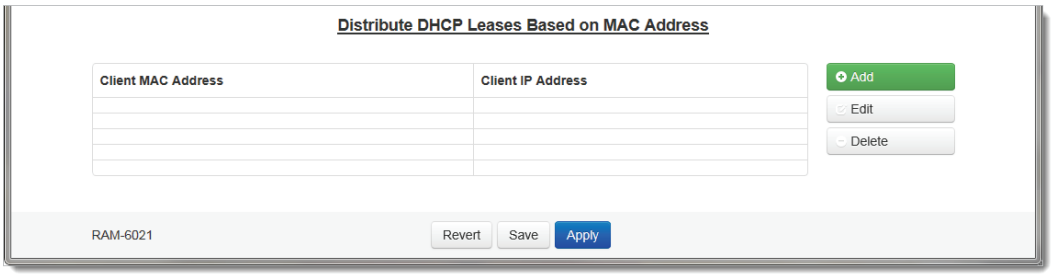
Recommended Setting: An address valid for the subnet for which the interface is configured. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Ending Address (Required Field): Enter the Ending IP Address of a range you want the DHCP Server to provide for clients.

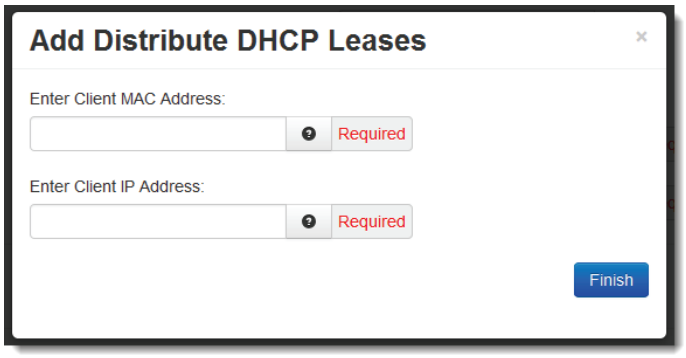
Recommended Setting: An address valid for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Care should be used to ensure that there is no conflict with any pre-existing devices on that sub-net which may have been already configured to use statically assigned IP addresses.

Show DHCP Leases: Click on the Show DHCP button to display the current DHCP leases logged on to the unit.

Distribute DHCP Leases Based on MAC Address:



- Click on the Add button to assign an IP Address to a device based on a MAC address, so that device obtains the same IP each time it requests a new IP from the DHCP server. The following window will appear:



Enter Client MAC Address (Required): This is the field where you enter the Client's computer or device MAC (Media Access Control) address.

The MAC address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable hardware identifier for the network.

When entering the MAC address information, type the 12-digit MAC address in the following format: xx:xx:xx:xx:xx:xx including the colons.

Enter Client IP Address (Required): Enter the IP address for which you wish to assign to a client's computer or device MAC address.

An address valid for the subnet for which the interface is configured. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to sue statically assigned IP addresses.

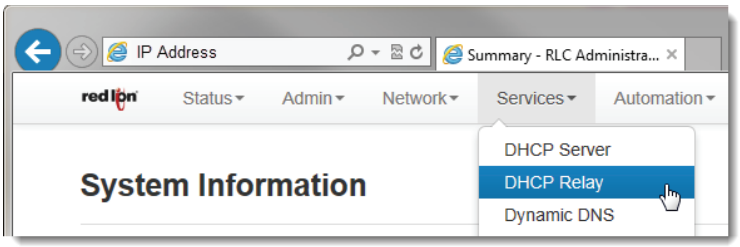
This address should have been provided by your Network Administrator.

- Click on the Finish button. You will return to the DHCP Server Settings dialog window and the entered data will be visible on the table at the bottom of the window.

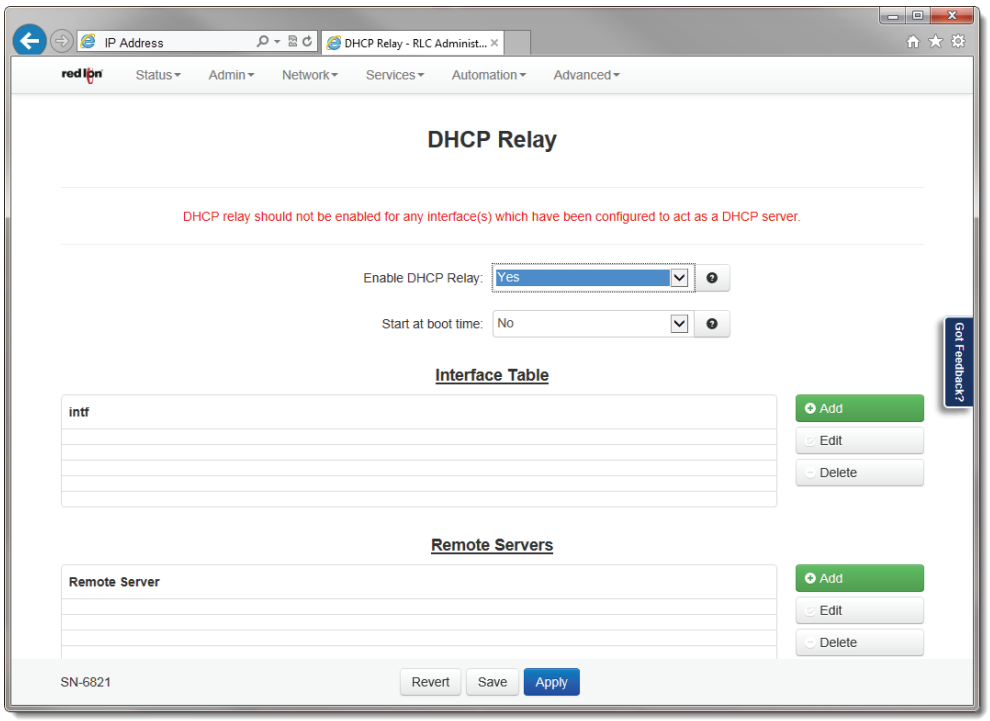
- To delete an address, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.5.2 DHCP Relay

This feature will enable a DHCP Relay service, which will connect a local interface with a remote DHCP Server. DHCP Relay should not be enabled for any interface(s) which have been configured to act as a DHCP server.



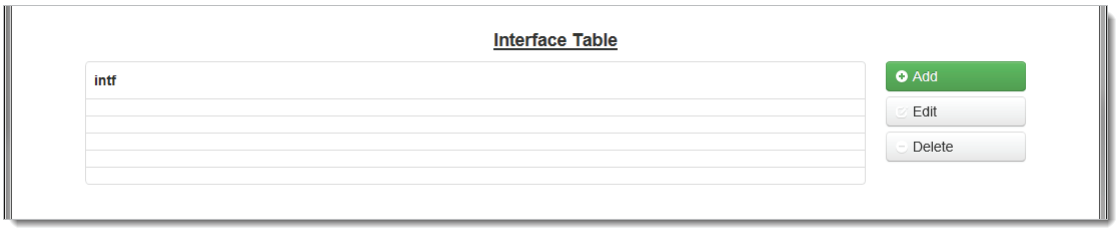
- Click on DHCP Relay and the following dialog window will appear:



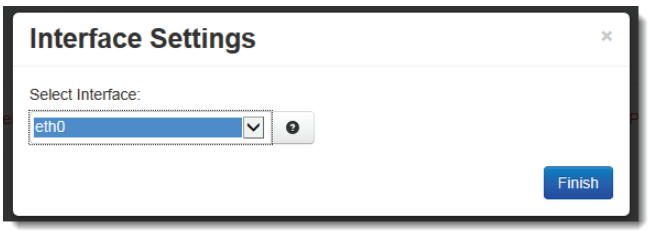
Enable DHCP Relay: Select YES to enable the DHCP Relay, or NO to disable it. The service will start once the Apply button is clicked. If the Save button is clicked, the service will not be started until the device is rebooted and then **only** if the *Start at boot time* option has also been set to YES.

Start at boot time: Select YES to enable the DHCP Relay at boot time, or NO for manual control. If the DHCP Relay service is required to be operational at all times, then set to YES. If another process, such as VRRP, is going to dynamically enable/disable DHCP Relay service as needed, then set to NO.

Interface Table:

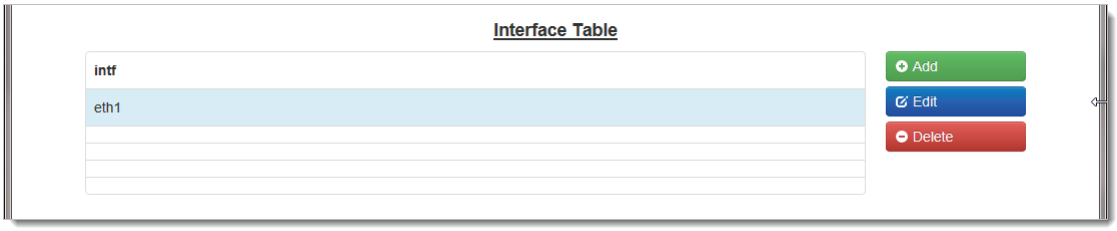


- Click on the ADD button and the following dialog window will appear:



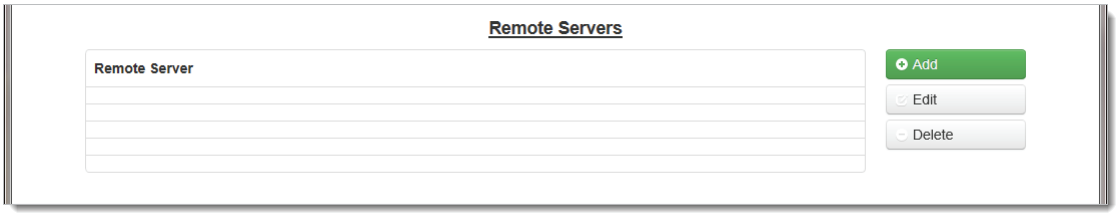
Select Interface: Select the interface to receive its IP from the remote DHCP server from the drop down menu.

- Click on the Finish button. You will be returned to the DHCP Relay dialog window and the Interface Table will be populated with the entered data.

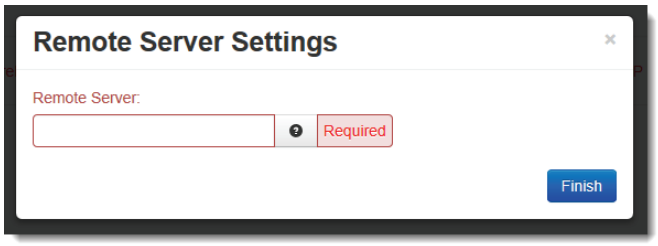


- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

Remote Servers:

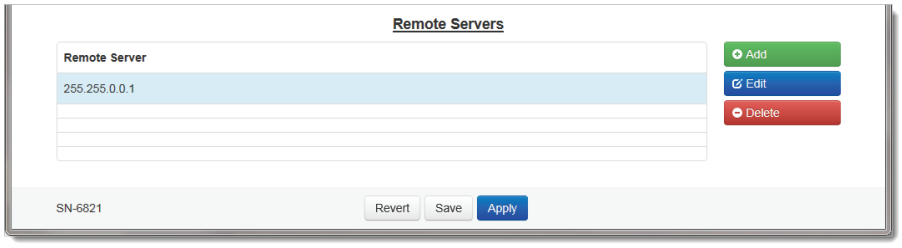


- Click on the ADD button and the following dialog window will appear:



Remote Server: Enter the IP Address or fully qualified domain name of all remote DHCP Servers available. It is the responsibility of the remote DHCP Server to coordinate the issuing DHCP addresses.

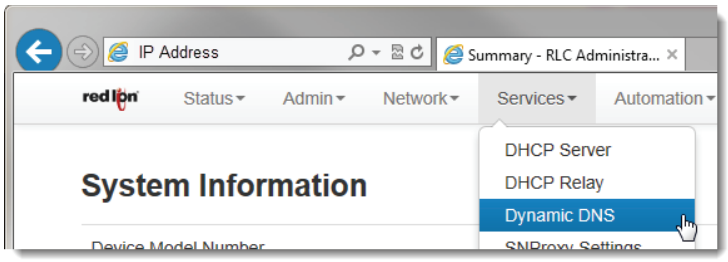
- Click on the Finish button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.



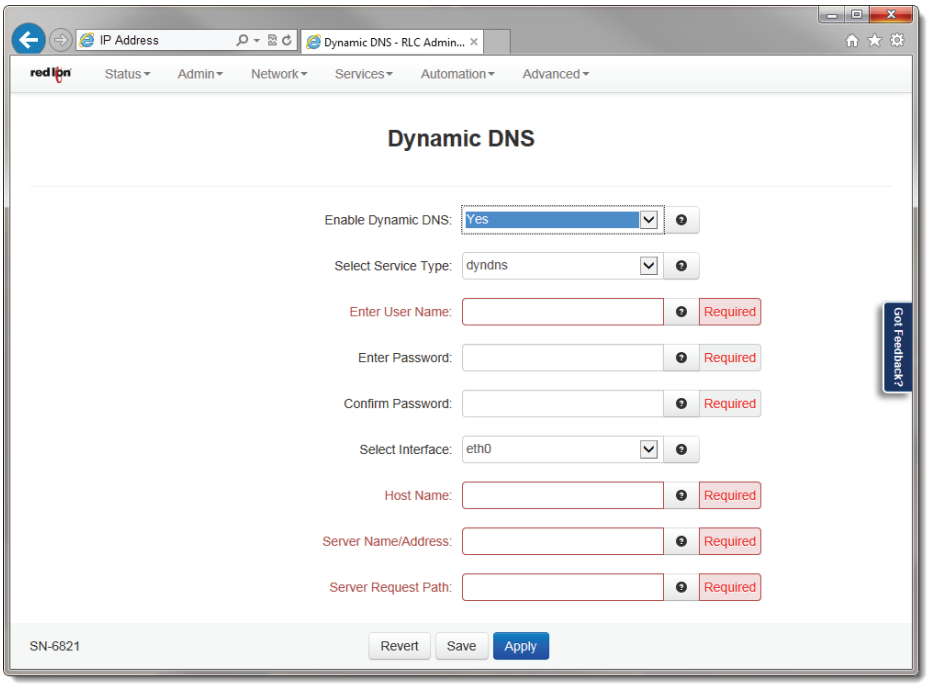
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.5.3 Dynamic DNS

The Dynamic DNS menu item is used to configure a dynamic DNS name for the Red Lion router that does not have a static public IP Address. A subscription to a service providing Dynamic DNS, such as DYNDNS.ORG, is required.



- Click on the Dynamic DNS menu item and the following dialog window will appear:



Enable Dynamic DNS: Select Yes to enable the Dynamic DNS Service.

Select Service Type: Select the desired Dynamic DNS Service from the list provided.

Enter User Name (Required): Enter the User Name used to access your Dynamic DNS Service in this field.

Enter Password (Required): Enter the password used to access your Dynamic DNS Service in this field.

Confirm Password (Required): Re-enter the password entered in the field above. The password must match exactly.

Select Interface: Specify the interface you want to access via Dynamic DNS. Changes made to the interface configuration after enabling Dynamic DNS will result in updates being sent to your Dynamic DNS service provider.

Host Name (Required): Enter the host name and domain you which to be assigned by the Dynamic DNS Service.

Server Name/Address (Required): Enter the host name or IP Address (along with port number, if needed) for user to access the Dynamic DNS Server. ***Example:*** *members. dyndns.com:80*

The recommended setting for this field is automatically displayed when you select a Service Provider. If you require a value other than the recommended value, your Network Administrator or Dynamic DNS Service Provider should be able to provide the appropriate value, which can be entered manually.

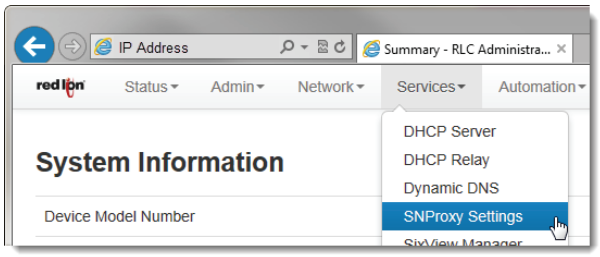
Server Request Path (Required): Enter the Request URL required to connect to the Dynamic DNS Service in this field.

The recommended setting for this field is automatically provided when a Service type is selected. If you require a value other than the recommended value, your Network Administrator or Dynamic DNS Service Provider should be able to provide the appropriate value, which can be entered manually.

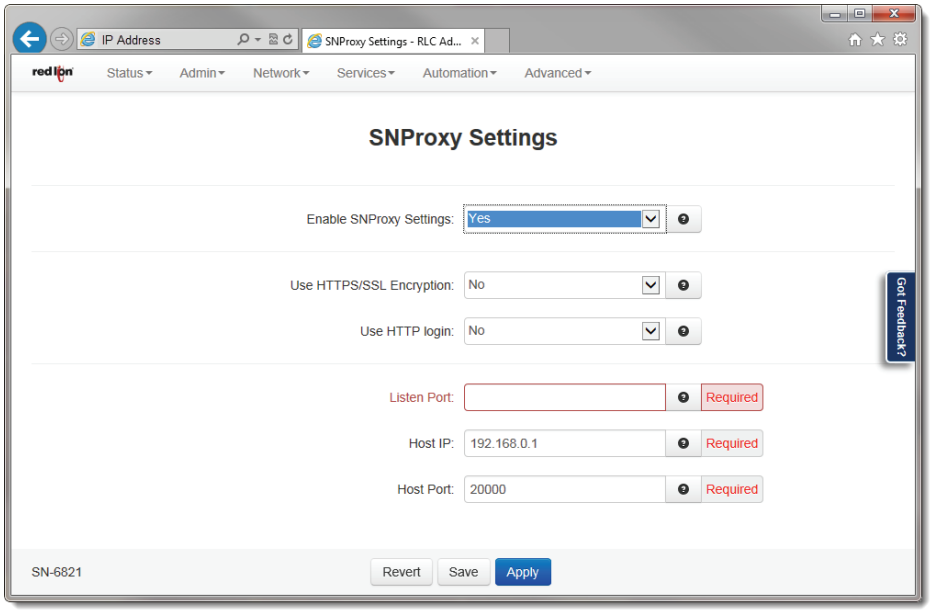
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.5.4 SN Proxy Settings

SN Proxy is a web relay proxy service used to gain access to devices that are behind our Red Lion router providing additional security and access control to devices that may not offer such functionality. A proxy based service provides a more robust connection than just using a port forward rule, including the ability to add an additional user login for authentication, encryption via SSL as well as isolation via Access Control Lists.



- Click on the SNProxy Settings menu item and the following dialog window will appear:



Enable SN Proxy Settings: Enables or disables the SN Proxy feature. If NO is selected, all other fields in the dialog window will be hidden.

Use HTTPS/SSL Encryption: Specify whether you want to enable the SSL engine for a more secure connection.

Use HTTP login: Specify whether you want to enable HTTP login. ***Note:*** *If you enable the HTTP login, you will be required to enter the username and password.*

Listen Port (Required): Enter the port number the SN Proxy listens for requests on.

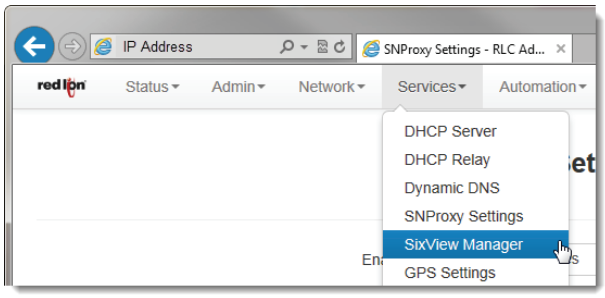
Host IP (Required): Enter the proxy server host IP address that will be accepting this connection request.

Host Port (Required): Enter the proxy server host port number.

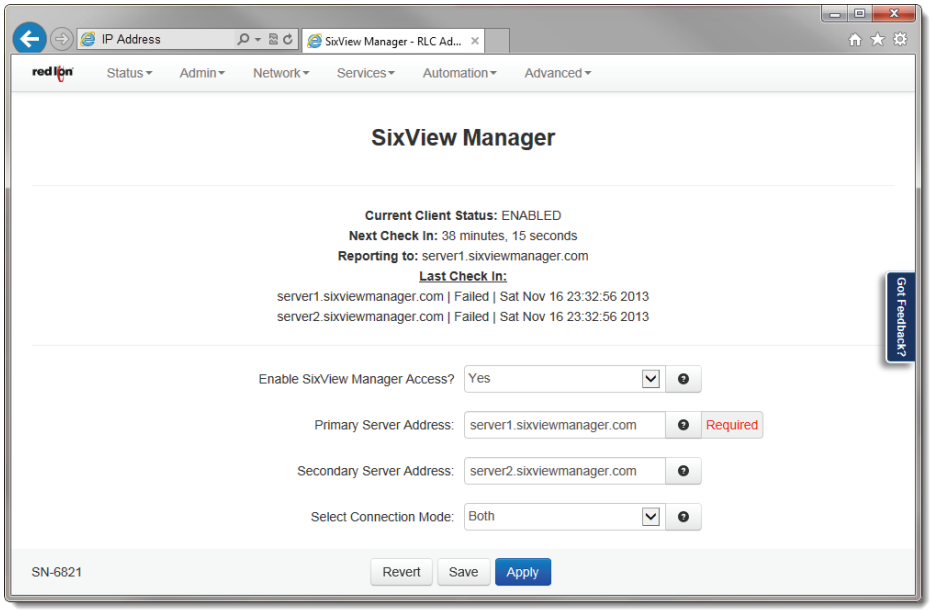
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to factory defaults.

3.5.5 SixView Manager

The SixView Manager menu item allows you to configure various aspects of the SixView Manager Client to communicate with a SixView Manager hosted at Red Lion or at your location.



- Click on the “SixView Manager” menu item and the following window will appear:



Enable SixView Manager Access: Select *Yes* to enable the SixView Manager Client, which will enable the device to communicate with the SixView Manager Server identified by the Host Address entered in the field below. To disable the SixView Manager Client, select *No* in the “Enable SixView Manager Access” pull down menu. All fields in the dialog window will disappear. The recommended setting for this field is *Yes*.

Note: A device managed by the SixView Manager Server may have its configuration altered at any time, without warning, so it is important to be aware of the actions the selected SixView Manager Server is configured to perform upon receiving a check-in from a new device before enabling this option. The recommended setting for this field is YES.

Primary Server Address (Required): Enter the IP Address or host name of your SixView Manager primary server.

When changing the Primary Address to your own private SixView Manager server, you may want to consider setting the Secondary Address to the Red Lion SixView Manager test server (server1.sixviewmanager.com) for trial and initial production rollouts This will enable Red Lion support staff to monitor the progress and better assist in diagnosing potential problems.

Secondary Server Address: Enter the IP Address or host name of your SixView Manager secondary server.

When changing the Primary Address to your own private SixView Manager server, you may want to consider setting the Secondary Address to the Red Lion SixView Manager test server (server2.sixviewmanager.com) for trial and initial production rollouts. This will enable Red Lion support staff to monitor the progress and better assist in diagnosing potential problems.

Select Connection Mode: Select the desired Connection Mode from the drop-down menu.

- **Primary Only:** The SixView Manager client only connects to the Primary Server.
- **Secondary Only:** The SixView Manager client only connects to the Secondary Server.
- **Both:** The SixView Manager client connects to the Primary and Secondary Servers.
- **Secondary when Primary unavailable:** The SixView Manager client preferentially connects to the Primary, using the Secondary as a backup.

The recommended setting is “Secondary when Primary unavailable” or “Both” are the preferred methods in configurations supporting redundant SixView Manager servers.

Enter Access Interval (minutes) (Required): Enter the number of minutes the SixView Manager Client process should wait before connecting to the SixView Manager server. A value of 220 is suggested for Cellular carriers that use an inactivity time out of four hours.

Note: While lower values can result in more timely status reports with the SixView Manager Server, it comes at an expense of increased data traffic, which may be an issue when the connection utilizes a cellular modem with a service plan where cost is based on bandwidth usage. A value of 220 is suggested for Cellular carriers that use an inactivity timeout of four hours.

Enter Error Interval (minutes) (Required): Enter the number of minutes the SixView Manager client should wait before re-attempting a previously failed check-in attempt. The recommended setting for this field is 30.

Select Access Method: Select the desired Access Method from the provided drop-down. There are two (2) access methods:

- **Unencrypted (http):** Faster, but less secure.
- **Encrypted (https):** Slower, but more secure.

Note that the encrypted method adds significant overhead which may be a consideration when using a cellular modem connection. For example, if an ipsec_restart is an option, then when selected, will be run whenever the fallback logic selects and activates this interface.

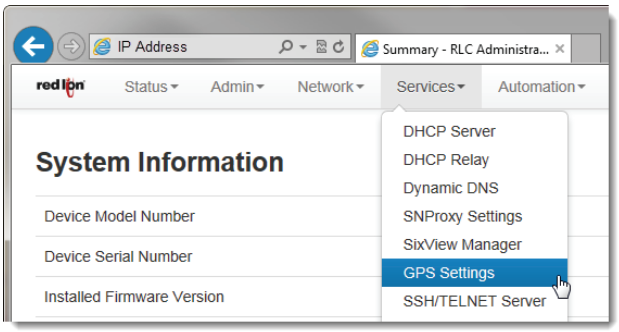
Enter SixView Manager Server Port # (Required): If the SixView Manager Server has been configured to accept connections on a port other than its standard default, that custom port number should be entered in this field. The administrator of the SixView Manager Server will be able to provide you with the necessary information to properly set this parameter. The recommended setting for this field is 18080.

Select Interface: Select the name of the interface to which the SixView Manager Client will bind for communications with the SixView Manager Server. The recommended setting for this field is *None*.

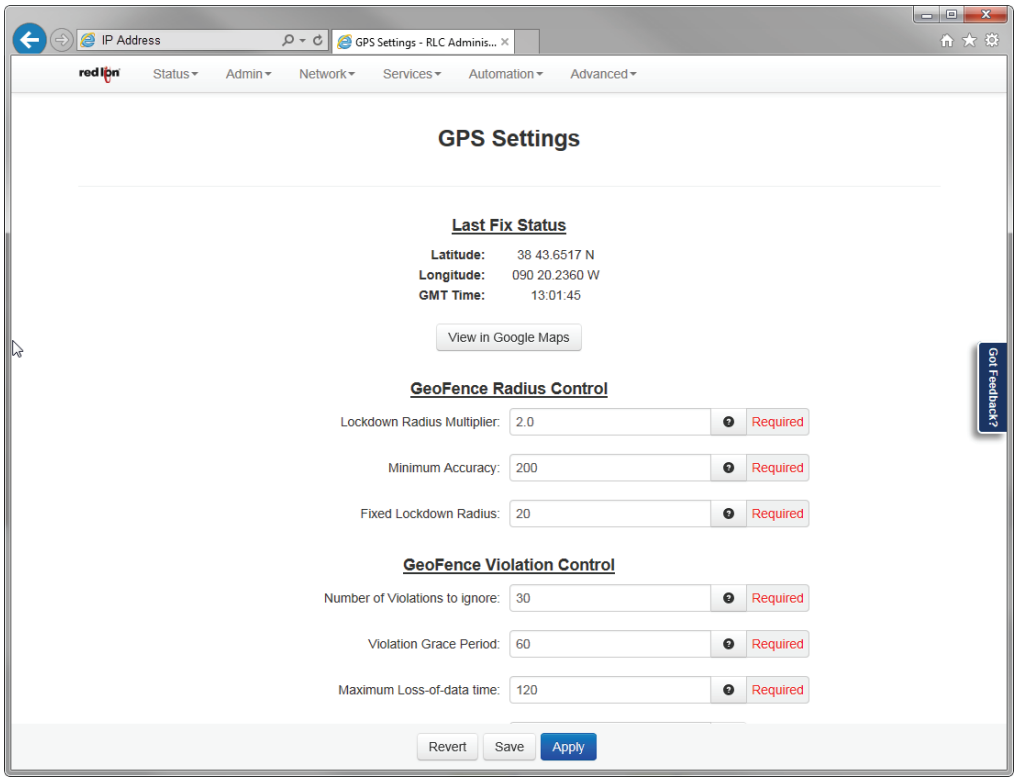
Note: This option will only be necessary if the SixView Manager Client is required to communicate through a configured IPSEC, GRE or IPIP tunnel.

- Click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to factory defaults.

3.5.6 GPS Settings



- Click on the GPS Settings menu item and the following dialog window will appear:



Lockdown Radius Multiple (Required): Enter the value of the Lockdown Radius Multiplier in this field. The recommended setting for this field is 2.

When the Geofence engine begins to build a fence, it will create a Calculated Minimum Radius allowed using an accuracy figure based on the acquisition 200 GPS location points obtained over an initial settling interval of about 15-20 minutes. This value is then multiplied by the Lockdown Radius Multiplier to obtain the Modified Minimum Radius.

The Modified Minimum Radius will not be allowed to become less than the Minimum Accuracy, and will be adjusted to the Minimum Accuracy as prevailing conditions require. The allowable range is 1.0 - 5.0.

Minimum Accuracy (Required): Enter the value of the Minimum Accuracy in this field. The recommended setting for this field is 50-200.

When the GeoFence engine begins to build a fence, it will calculate an allowed Minimum Radius using an accuracy figure based on an average of 200 location points acquired over an interval of 15-20 minutes. This value is then multiplied by the Lockdown Radius Multiplier to obtain the Modified Minimum Radius.

The Modified Minimum Radius will not be allowed to be less than the Minimum Accuracy, and will be increased to the Minimum Accuracy as needed. The Minimum Accuracy will also provide a lower limit for the Fixed Lockdown Radius. The allowable range is 0-2000.

Fixed Lockdown Radius (Required): The value of the Fixed Lockdown Radius may be entered in this field. The recommended setting for this option is 0 (off).

GeoFence behavior can be described in the following ways:

- **Flexible radius**: To select this option, the Fixed Lockdown Radius must be set to **0**.
- **Flexible radius with additional fixed buffer:** To select this option, enter a value, preceded with '**+**'.
- **Fixed radius:** To select this option, enter any non-zero value.

During the establishment of a GeoFence, a set of 200 location points are obtained over a period of 15-20 minutes to determine an initial 'minimum radius' possible for the device. The Flexible radius behavior uses the *Calculated Minimum Radius* and the configured *Lockdown Radius Multiplier* values to set the GeoFence boundary. Setting the *Fixed Lockdown Radius* to a positive offset (+20, for example) has the effect of adding a fixed amount of buffer space to the *Calculated Minimum Radius*, and the *Lockdown Radius Multiplier* has no effect.

For Fixed Radius behavior, the configured value for the *Fixed Lockdown Radius* is used to set an absolute minimum radius for the GeoFence, subject to increase by the configured *Minimum Accuracy* or *Calculated Minimum Radius* values as needed.

Note that since the calculated minimum radius may change over time depending on acquired GPS location data, the value will never be allowed to become less than the *Minimum Accuracy* nor the *Calculated Minimum Accuracy*.

Number of Violations to ignore (Required): Enter the number of violations to ignore in this field. The recommended value for this field is 10-30 points (approximately 20-60 seconds).

To limit false alarms from occasional drifting GPS points, this value will ignore a certain number of anomalous points before alerting a SixView Manager server. This prevents an inaccurate site from constantly updating the SixView Manager with dubious information. New points are received about every 2 seconds. The allowable range is 0-300.

Violation Grace Period (Required): The value of the Grace Period may be entered in this field. The recommended setting for this field is 60.

Once we have ignored the first few anomalous location fixes, points outside the GeoFence are considered a **violation**. This timer specified (in seconds) how long to tolerate points outside the GeoFence boundary, before declaring a full "Violation Outside" and enacting the "Violation Action". The allowable range is 30-600.

Maximum Loss-of-data time (Required): The maximum number of seconds for which no GPS data is received may be entered in this field. The recommended setting for this field is 120.

Ordinarily, a GPS device generates location information updates on a continuous regular periodic basis. A loss of these updates may be due to a temporary or intermittent reception issue, or due to the device having been moved to an area devoid of GPS reception or disconnection or an external GPS receiver, either deliberately or accidentally by persons authorized to do so or not.

This parameter sets the period of GPS data loss beyond which the device may be considered having been tampered with and subject to securing actions. The allowable range is 30-1200.

Select Violation Action: Select the action to be taken when a protected perimeter violation occurs using the drop-down list provided. The available options are:

- **Custom:** Configured special actions are applied:
- **Block All:** In addition to the actions taken in Block Network, all access to the device including via physical ports (console, etc.) is blocked.
- **Block Network:** All network traffic, except to a SixView Manager server, will be blocked.
- **Report Only:** The device reports violation events to a SixView Manager server.

Configure Advanced GPS Parameters: Select Yes to configure advanced GPS parameters.

Valid Points Required (Required): The maximum number of valid GPS location entries required for GeoFence boundary establishment may be entered in this field. The recommended setting for this field is 200.

This configures the number of GPS Data points to collect before building the GeoFence boundary. These points are collected when instructed to go into initial Lockdown mode. Larger values require more time to build the initial fence, yet may yield a more accurate Calculated Minimum Radius. The allowable range is 100-1000.

Distance Reporting Threshold (Required): The value for the Distance Reporting Threshold may be entered in this field.

When not in GeoFence Lockdown, a Distance Threshold exceeded message will be sent to a SixView Manager server every time the unit is moved more than the configured amount (in feet) from its previously recorded location. This is typically only useful in a mobile application. The allowable range is 200-1000000 (feet).

Require User Cleared Violations: Select whether the user is required to clear perimeter violations using the drop-down list provided. The recommended setting for this field is 0. Available values are:

- No
- Yes

Whenever a full violation state has been reached (Violation Outside or Violation No Data), the next good GPS data point received will automatically clear the violation and return the unit to “Lockdown Good”. When this option is set to Yes, then the Violation will NOT be cleared until a SixView Manager server or user sends down a command to re-initiate Lockdown. This will build a new GeoFence boundary based on current location and radius parameters.

Maximum log entries (Required): The value for Maximum log size may be entered in this field. The recommended value for this field is 600.

Number of log entries to keep in a GPS raw log in NMEA format. Raw GPS Log access is available upon request. A new log entry will be generated according to the setting in Raw Log Interval. A maximum of 50k is saved. The allowable range is 100-1000.

Discardable # outlier points (Required): The value of the # Outlier Points to Ignore may be entered in this field. The recommended setting for this field is 5.

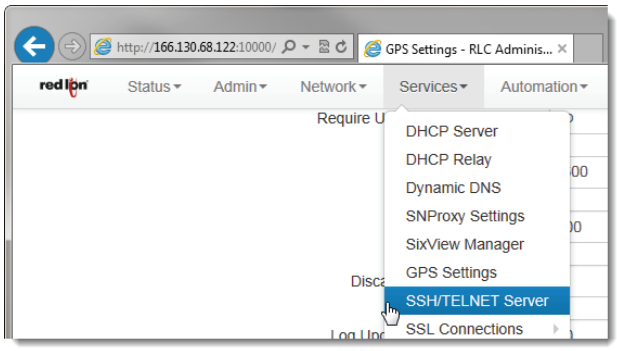
When a GeoFence is being established, the GPS engine ignores a certain number of the first few anomalous location fixes before points outside the GeoFence are subject to **violation** actions. After that initial ‘settling period’, each new GPS point must be examined in relation to the established boundary. Even under ideal conditions, intermittent signal reception and/or multipath interferences issues can result in points being erroneously reported beyond the GeoFence boundary. This parameter can be used to tune the filtering of this ‘jitter’ to reduce the likelihood of a false positive GeoFence violation. The allowable range is 0-50.

Log Update Interval (seconds): This parameter determines how often (in seconds) the current GPS data point will be saved in NMEA format in a Raw GPS logfile. The allowable range is 5-10000.

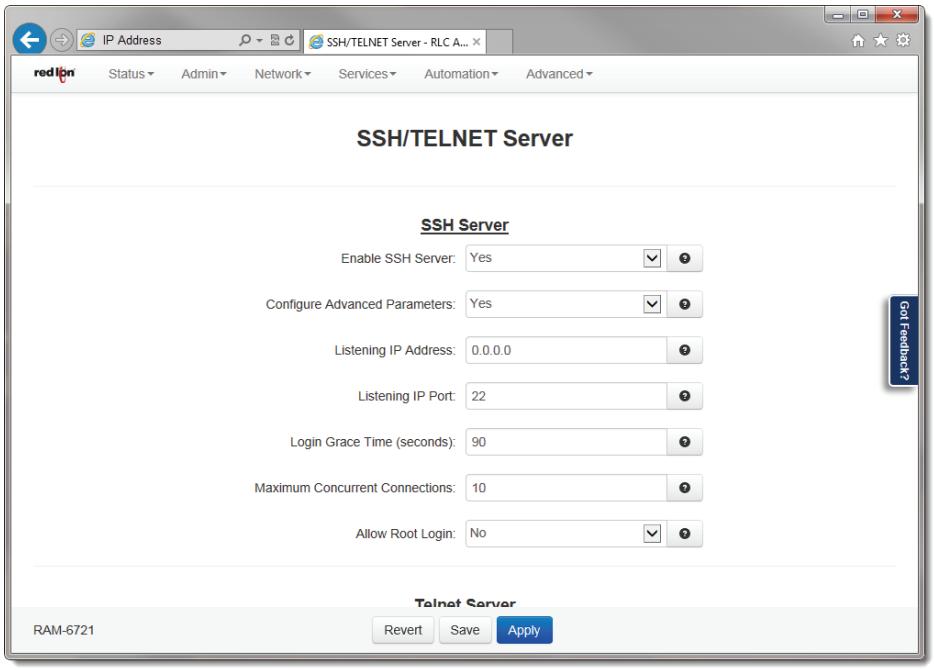
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to factory defaults.

3.5.7 SSH/TELNET Server

The SSH/TELNET Server menu allows you to configure whether the Red Lion router will communicate with the network via Secure Shell (SSH) and to enable or disable TELNET on the Red Lion router.



- Click on the SSH/TELNET menu item and the following dialog window will appear:



SSH Server

Enable SSH Server: Select YES to enable the SSH server. *Note:* Enabling the SSH Server does not, by default, allow SSH data through the firewall. If you have connection problems, please check your firewall settings.

Configure Advanced Parameters: Select YES to configure advanced options for the SSH Server (Optional). The recommended setting for this field is NO.

Listening IP Address: Specifies the local IP Address on which the SSH server will accept connections. *Note:* Specifying a value of 0.0.0.0 allows the SSH server to accept connections on any interface. Firewall rules must be present to allow SSH connection on untrusted interfaces. The recommended setting for this field is 0.0.0.0.

Listening IP Port: Specifies the local IP port on which the SSH server will accept connections. *Note:* Specifying a value other than 22 will require proper firewall rules in order to allow connections to the given port. The recommended setting for this field is 22.

Login Grace Time (seconds): Specifies the amount of time, in seconds, after which the SSH server will disconnect, if the user has not successfully logged in. The recommended setting for this field is 30.

Maximum Concurrent Connections: Specifies the maximum number of concurrent unauthenticated connections to the SHH server. Additional connections will be dropped until authentication succeeds, or the Login Grace Time expires for a connection. The recommended setting for this field is 10.

Allow Root Login: Specifies whether root can log in directly to the SSH server. The recommended setting for this field is *No*.

Telnet Server

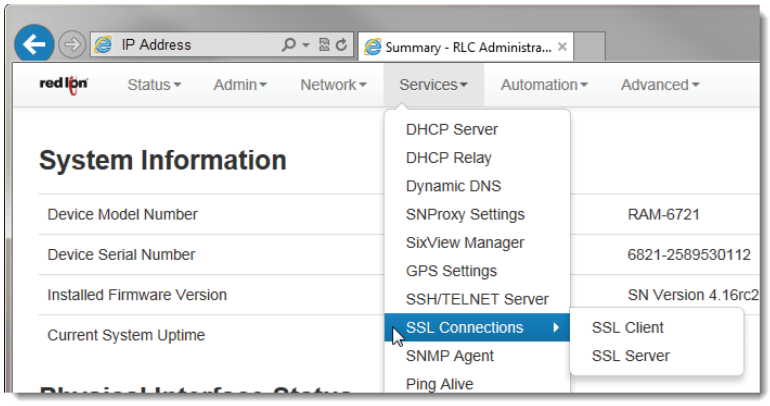
Enable Telnet Server: Select YES to enable the Telnet Server. *Note:* Enabling the Telnet Server does not, by default, allow Telnet data through the firewall. If you have connection problems, please check your firewall settings.

The recommended setting for this field is NO.

- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

3.5.8 SSL Connections

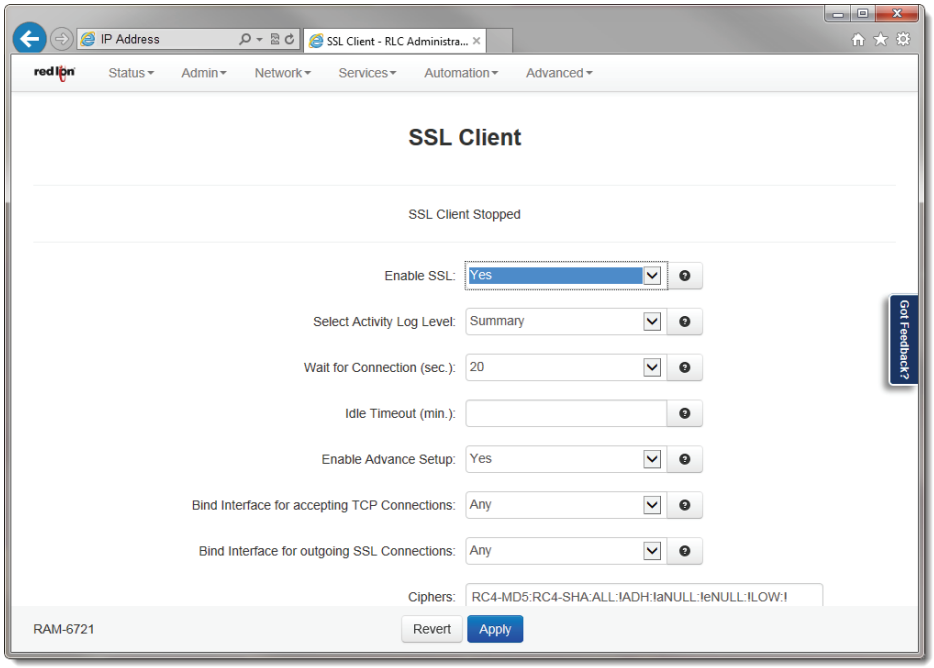
The SSL Connections menu item is used to configure the Red Lion router to either act as a Secure Socket Layer (SSL) Client to receive certificates or as an SSL Server to issue certificates. The SSL Connections tab is sub-sectioned into the SSL Client and the SSL Server.



3.5.8.1 SSL Client

The SSL Client menu item is used to configure the Red Lion router to be a SSL client and receive a certificate of authorization from an SSL server to authenticate connections for secure communications.

- Click on the SSL Client menu item and the following dialog window will appear:



Enable SSL: Select Yes to configure SSL client/server. Select No and then the Apply button to disable SSL.

Select Activity Log Level: This option controls the logging level for SSL Connection activity. The recommended setting for a production environment is: Summary. For a test environment: Full.

Wait for Connection (sec.): Time (in seconds) allowed after sending SYN packets, to wait for SYN-ACK. The recommended setting for this field is 20 seconds.

Idle Timeout (min): Time (in minutes) allowed for no traffic over an SSL connection, before closing down the link. The recommended setting for this field is 720 (minutes).

Enable Advance Setup: Select Yes to modify advanced SSL options.

Bind Interface for accepting TCP Connections: This will restrict the unencrypted listening socket to allow connections coming into the specified interface only. The recommended setting for this field is *Any*.

Bind Interface for outgoing SSL Connections: This will restrict the encrypted socket to initiate connections out the specified interface only. Specifying an interface here may conflict with policy routing, however it may be required in a GRE/VPN or other tunneled environment. Please consult with a network architect for additional assistance. The recommended setting for this field is *Any*.

Ciphers: This field is a list of supported openssl ciphers. Please consult support staff before attempting to change these values. Reference Google: “openssl cipher list” for more information. The recommended setting for this field is: RC4-MD5:RC5-SHA:SSLv3

Select Certificate: Specifying a certificate in client mode will use this certificate chain as a client side certificate chain. Using client side certs is optional. The certificates must be in PEM format, with an unencrypted key (not password protected when generated). Use Admin->Certificate Manager to install/update certs.

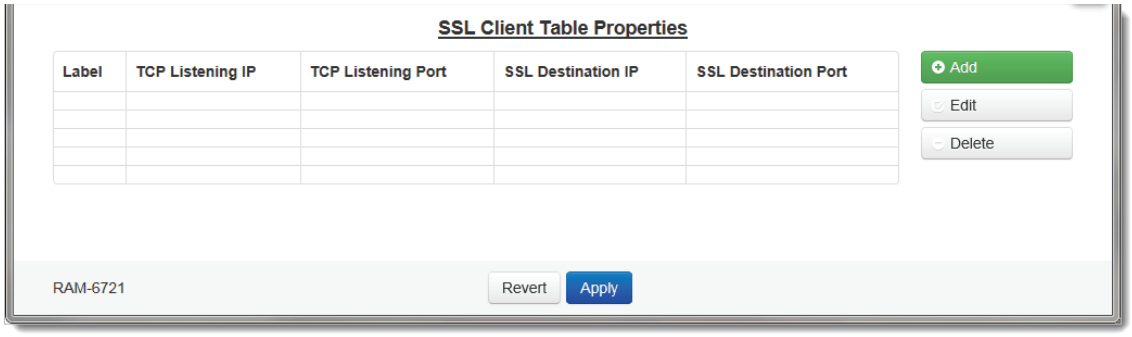
Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

- **None:** Keep-alives not used.
- **All:** Keep-alives enabled for all sockets.
- **Accept:** Keep-alives enabled for listening server socket side connections only. This applies to the clear text server for Client mode sockets, or the SSL Encrypted server for Server mode sockets.
- **Remote:** Keep-alives enabled for client initiated sockets.
- **Local:** Keep-alives enabled for Client connections bound to a local IP address.

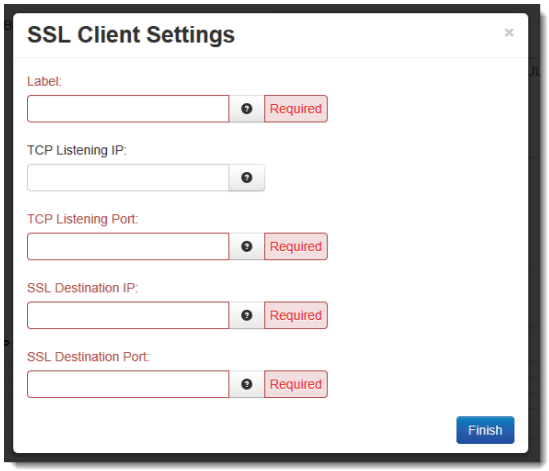
You may need to adjust the master Keep-alive timer via Network->TCP Global Settings->TCP Keep Alives.

Note: Enabling TCP keep-alives may dramatically increase the total amount of traffic for the affected socket(s) depending on the master interval, probe and timeout settings, which should be considered for connections using a wireless (cellular) connection with respect to total data usage for the subscripted plan.

SSL Client Table Properties:



- Click on the Add button and the following dialog window will appear:



Label (Required): Enter a unique name to describe this connection.

TCP Listening IP: Enter the IP to listen on for incoming connections. If not using static IP addresses, it is recommended to use the Advanced Setup option “Bind Interface for accepting TCP Connections” instead. The recommended settings for this field are:

- Leave Blank (0.0.0.0) to allow connections from any interface.
- Use 127.0.0.1 for internal connection use only (gwlnx Protocol Converter).

TCP Listening Port (Required): Enter the listening port for this connection. Please note that this port must be allowed in the Firewall access rules for any external/untrusted interface. It may be useful to review the results of ***Status->Network->Socket Statuses->TCP Only*** to confirm that your choice of listening port is not already in use. (Ports under "Local Address" with a state of "Listen" are in use.)

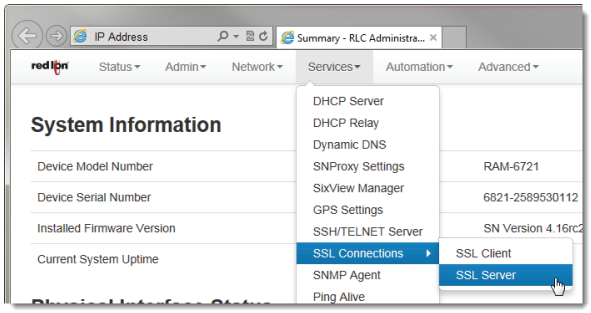
SSL Destination IP (Required): Enter the IP or Domain Name of the SSL server to which you would like to connect.

SSL Destination Port (Required): Enter the Port number of the SSL server to which you would like to connect.

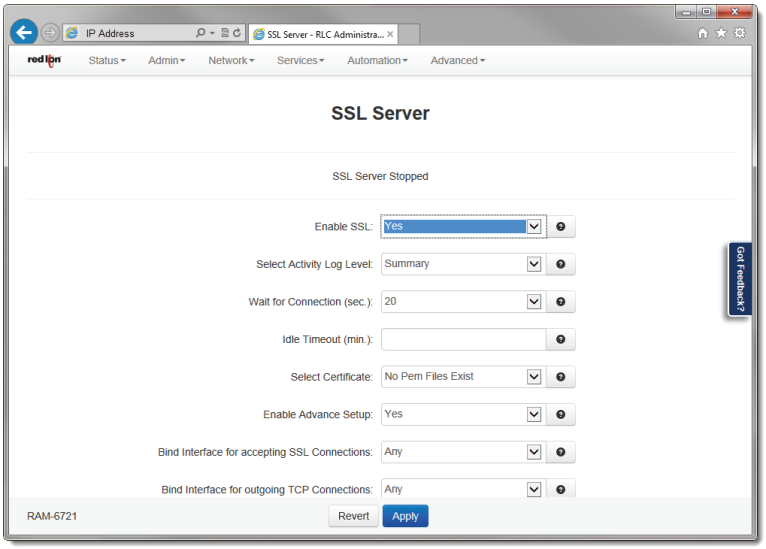
- Click on the Finish button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.
- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

3.5.8.2 SSL Server

The SSL Server menu item is used to configure the Red Lion router to issue SSL certificates to requesting SSL clients.



- Click on the SSL Server menu item and the following dialog window will appear:



Enable SSL: Select Yes to configure SSL client/server. Select No and click the Apply button to disable SSL.

Select Activity Log Level: This controls the logging level for SSL Connection activity. The recommended setting for a production environment is *Summary*. The recommended setting for a test environment is *Full*.

Wait for Connection (sec.): Time (in seconds) allowed after sending SYN packets, to wait for SYN-ACK. The recommended setting for this field is 20 seconds.

Idle Timeout (min.): Time (in minutes) allowed for no traffic over an SSL connection, before closing down the link. The recommended setting is 720 minutes.

Select Certificate: A server certificate must be provided. This will be used to encrypt communication with all clients. The certificates must be in PEM format, with an unencrypted key (not password protected when generated). Self signed certificates are highly recommended. Use Admin->Certificate Manager to install/update certs.

Enable Advanced Setup: Select Yes to modify advanced SSL options.

Bind Interface for accepting SSL Connections: This will restrict the encrypted listening socket to allow connections coming into the specified interface only. The recommended setting for this field is *Any*.

Bind Interface for outgoing TCP Connections: This will restrict the unencrypted socket to initiate connections out the specified interface only. Specifying an interface here may conflict with policy routing, however it may be required in a GRE/VPN or other tunneled environment. Please consult with a network architect for additional assistance. The recommended setting for this field is *Any*.

Ciphers: This field is a list of openssl ciphers supported. Please consult support staff before attempting to change. Reference Google:”open ssl cipher list” for more information. The recommended settings for this field are: RC4-MD5:RC4-SHA:SSLv3.

Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

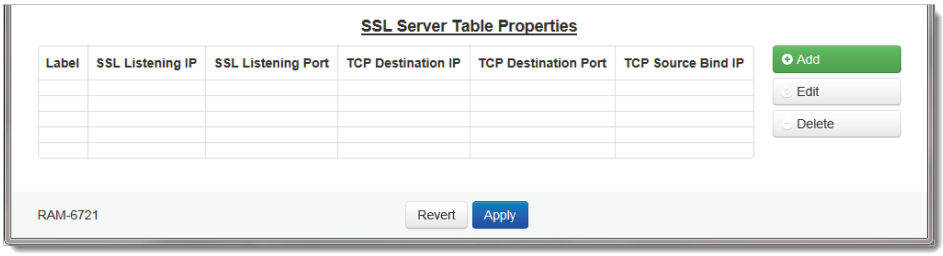
Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

- **None:** Keep-alives not used.
- **All:** Keep-alives enabled for all sockets.
- **Accept:** Keep-alives enabled for listening server socket side connections only. This applies to the clear text server for Client mode sockets, or the SSL Encrypted server for Server mode sockets.
- **Remote:** Keep-alives enabled for client initiated sockets.
- **Local:** Keep-alives enabled for Client connections bound to a local IP address.

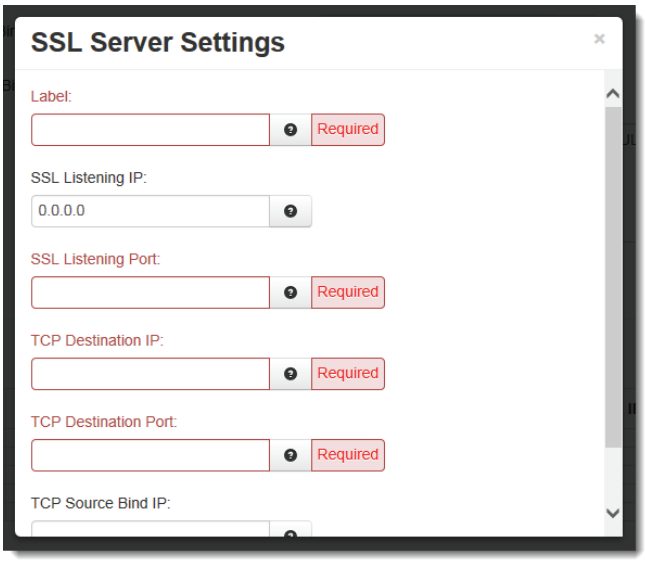
You may need to adjust the master Keep-alive timer via Network->TCP Global Settings->TCP Keep Alives.

Note: Enabling TCP keep-alives may dramatically increase the total amount of traffic for the affected socket(s) depending on the master interval, probe and timeout settings, which should be considered for connections using a wireless (cellular) connection with respect to total data usage for the subscripted plan.

SSL Server Table Properties:



- Click on the Add button and the following dialog window will appear:



Label (Required): Enter a unique name to describe this connection.

SSL Listening IP: Enter the IP to listen on for incoming SSL connections. If not using static IP addresses, it is recommended to use the Advanced Setup option “Bind Interface for accepting TCP Connections” instead. The recommended setting for this field is to leave it blank (0.0.0.0) to allow connections from any interface.

SSL Listening Port (Required): Enter the listening port for SSL connections. Please note that this port must be allowed in the Firewall access rules for any external/untrusted interface. It may be helpful to review the results of Status->Network->Socket Statuses->TCP Only to confirm that your choice of listening port is not already in use. (Ports under “Local Address” with a stat of “LISTEN” are in use.)

TCP Destination IP (Required): Enter the IP or Domain Name of the standard TCP server to which you would like to connect. Use 127.0.0.1 for internal connection use only (gwlnx Protocol Converter, or OOB Encryption Setup).

TCP Destination Port (Required): Enter the Port number of the standard TCP server to which you would like to connect.

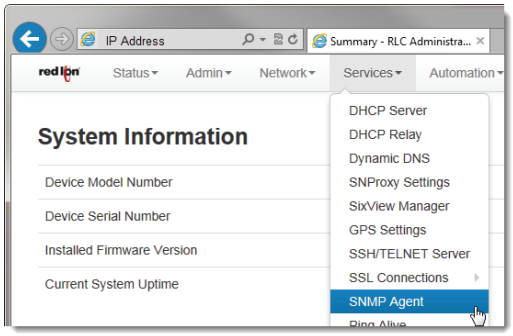
TCP Source Bind IP: Enter the IP to bind for outgoing TCP connections. If not using static IP addresses, it is recommended to use the Advanced option “Bind Interface for outgoing TCP Connections”. The recommended setting for this field is to leave it blank for normal operation (no binding).

- Click on the Finish button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.

- To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

3.5.9 SNMP Agent

SNMP (Simple Network Management Protocol) is an industry standard way of querying networking devices to obtain statuses, updates, alerts and behaviors.



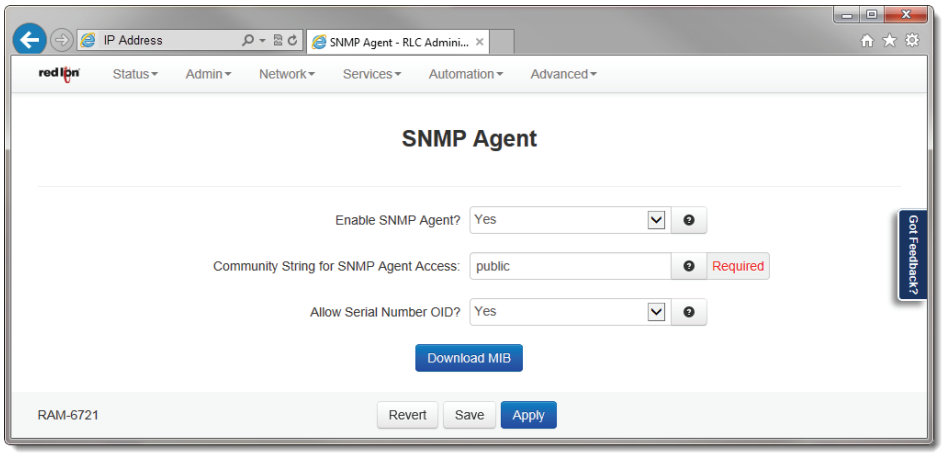
To retrieve SNMP data from the Red Lion device you must have an SNMP manager or Server at the head end. The Red Lion router will only act as an SNMP client, providing data it is polled for. It will not act as a manager to poll other devices.

The SNMP Agent allows you to query the unit for information via SNMP using what is called a MIB (Management Information Base). Standard MIB-II queries are supported, as well as a custom RED-LION-RAM.MIB. A great deal of useful information about the unit interface, including cellular signal strength, interface status, and more can be queried. When configuring firewalls to allow SNMP traffic, be sure to allow access to port 161 so that the device may return its results. This is the industry standard port number for SNMP traffic.

A complete listing of the OIDs found in the RED-LION-RAM.MIB can be found in the Appendix at the end of this manual.

* The community string is “public” (do not enter the quotes).

- Click on the “SNMP Agent” menu item and the following dialog window will appear:



Enable SNMP Agent: Select YES to enable the SNMP Agent. Note: Enabling the SNMP Agent does not, by default, allow SNMP data through the firewall. If you have connection problems, please check your firewall settings.

Community String for SNMP Agent Access (Required): Specify the community string to use for authentication between the SNMP Agent and Manager. Alpha-numeric strings are supported. Note: The community string must match on both ends of the connection in order to work.

Our default community string for the RED-LION-RAM.MIB is “public”.

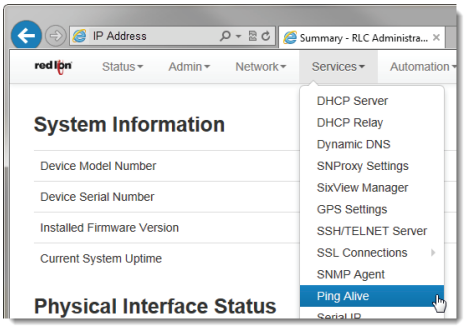
Allow Serial Number OID: Select YES to allow users and management systems to retrieve the unit serial number from the SNMP Agent. If NO is selected, a query of the serial number OID will return “UNKNOWN”.

Download MIB: Click on this button to download the MIB file.

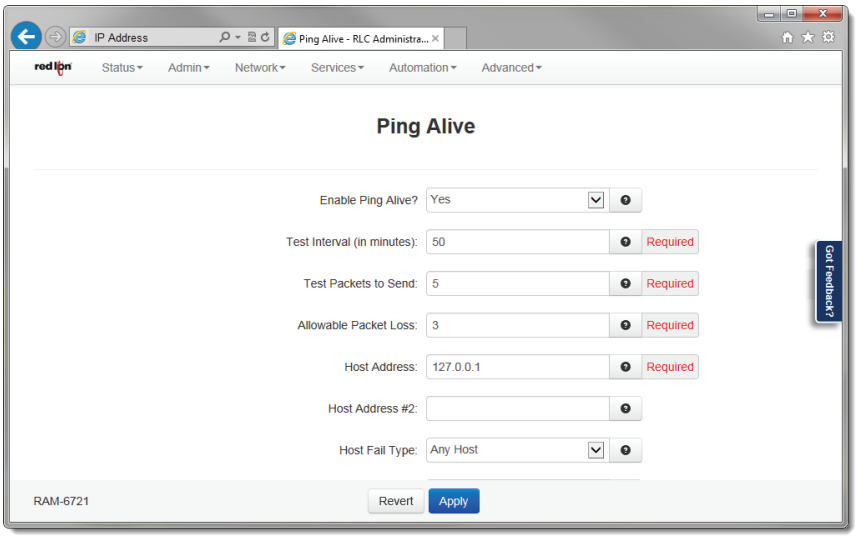
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

3.5.10 Ping Alive

Ping is a diagnostic tool used for verifying connectivity between two hosts on a network. It sends ICMP (Internet Control Message Protocol) echo request packets to a remote IP address and watches for ICMP responses.



- Select the Ping Alive tab menu and the following dialog window will appear:



Enable Ping Alive: Select YES to enable the Ping Alive Service. The recommended setting for this option is NO. Ping Alive will send the specified number of packets in Test Packets to Send, every interval defined in Test Interval. Should the ping fail to the first host, a second host may also be defined. Host Fail Type will control how many hosts must fail before a failure is declared and Failure Command Script will execute the failure action specified at that time. This can be used to force interface traffic, or to probe connectivity to an end point.

Test Interval (in minutes)(Required): Enter the time interval (in minutes) to which the ping packets would be sent. The recommended setting for this option is 50.

Test Packets to Send (Required): Specify the number the time packets to send out to test connectivity. The minimum is 1 and the maximum is 10. The recommended setting for this field is 5 - 10.

Allowable Packet Loss (Required): Specify the number of lost packets that are acceptable before the link is considered unavailable. Note: The value must be less that the number of test packets set via Test Packets to Send. Example: If Test Packets to Send is set to 5 and Allowable Packet Loss is set to 3, then 2 pings of the 5 sent out must have replies for connectivity to be declared successful. If only 1 ping reply is received, then a failure to that host will be declared.

Host Address (Required): Enter the IP Address of the destination host to which the ping packet would be sent. Default setting is “127.0.0.1”.

Host Address #2: Enter the IP Address of the second destination host to which the ping packet would be sent. This second host is tested only when the first one fails. There is no default setting for this option.

Host Fail Type: Choose “Any Host” to run the action when the first and last host fail the test. Choose “Last Host” to run the action when the first and lost host fail the test. Host Address #2 is only tested if the first host fails.

Source Interface: Select the name of the interface to which the service will bind for communications tests. When set to *None*, the system will choose automatically. The recommended setting for this option is None.

Source IP Address: Enter the IP address to use as a source for communications tests. Note: This will be the source IP address of the PING packets, but does not necessarily reflect the interface from which packet will traverse the unit.

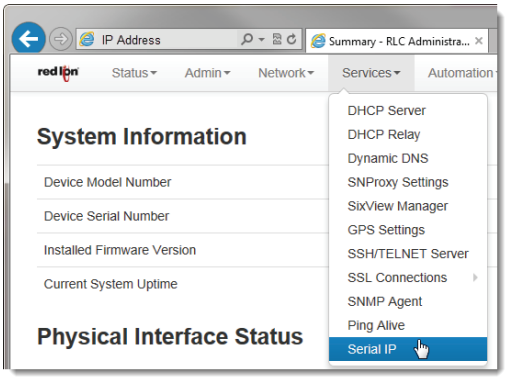
Failure Command Script: Choose the name of the command script to be executed when the PING test fails. For example, if “Restart Wireless” is an option, then when selected, the wireless interface will be restarted.

Note: Recommended setting is “*None*” for standard operation with no special behaviors. “*RestartWireless*” is useful when using a wireless (cellular) interface. “*Reboot*” will restart the entire device.

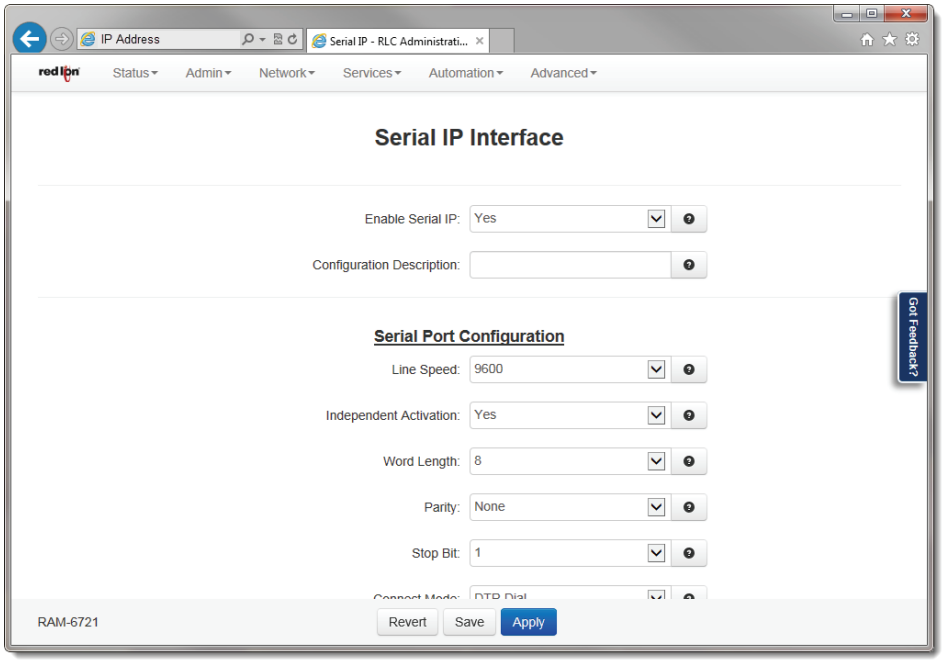
- Click on the APPLY button for the changes to take effect. Selecting Revert, will reset all fields to previously saved defaults.

3.5.11 Serial IP

The Serial IP menu item is used to configure serial communication such as POS device, serial data logging or serial transmitter via serial cable on the Red Lion router and third party UDP or TCP/IP Client/Server application.



- Select the Serial IP menu item and the following dialog window will appear:



Enable Serial IP: Select Yes to enable the Serial IP interface.

Configuration Description: Enter a description to describe the intent of this communication. Character limit is 128.

Line Speed: Select the desired interface speed to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Independent Activation: This option determines if the Serial Port of the device will accept data before the remote side is active. At least one of the two sides in the configuration must be set for Independent Activation. If neither side is set, then the device will not accept date. This function provides integrity for the device by preventing data from being accepted until it can be delivered successfully.

Select *Yes* for standard usage. Select *No* for serial to TCP Server configuration to insure there is a TCP Server socket available before marking the serial port active. Select *Negotiate* only if directed by Red Lion Technical Support.

Word Length: Select the word length (bits per character) to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Parity: Select the parity to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Stop Bit: Select the number of stop bits to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Connect Mode: If this option is set to No, the device will expect to receive AT Commands in order to go to active state. Some DTE (Data Terminal Equipment) devices required to go active if they provide DTR (Data Terminal Ready) signal. The recommended setting for this field is *Yes*, if DTR is the connect signal.

Ignore DTR: This option needs to be set to Yes, if the serial port is connected to a DTE device that only provides 3 wires (Transmit, Receive and Ground) for communication or the DTE device could drop DTR signal while sending AT commands. The recommended setting for this field is *YES* if 3 wires connection is expected.

Connection Type: Select the connection type you desire from the drop-down list. The recommended setting for this field is Modem Emulator for direct connection.

Modem Emulator: Provided direct connection between the device serial port and the DTE terminal via straight RS232 cable.

Via Modem: This option is only used if the device provides TELCO/BPX or RJ11 To Terminal port for communication.

Use Timer Only: This option needs to be set to Yes in order to use the Inter Character Timeout value configured on this device. The recommended value for this field is *Yes*.

Inter Character Timeout (ms): When the timer expires on the serial port, the device will forward the message received to the remote device. This option is used when there is no consistent character to signal the end of a received message. This timer will be reset to the configured value on each received character. The recommended value for this field is 5 milliseconds at 9600 baud.

Maximum Buffer Size: Set the maximum buffer size to be used for receiving serial data before forwarding to the remote device. A value of 0 will allocate 8192 bytes of buffer by default and the data could be sent to the remote application based on TCP stack window size. The recommended setting for this field is 292 for DNP3 type connections and 0 for all other connections.

Enable Hardware Flow Control: Select Yes to set hardware flow control using RTS and CTS signals. The recommended settings for this field are: *No* if dealing with 3 wires port (Transmit, Receive and Ground pins), *Yes* if dealing with the port that have all their signal pins present.

Number of Missed Polls Allowed: Set the maximum number of missed RTU polls before re-initializing all the internal memory and buffer conditions. If a packet is transmitted out the serial port and no response packet is received, this is counted as a missed poll and data content is not evaluated. The recommended setting for this field is 0, to disable this action. Any other value is upon your environment requirements.

Socket Type: Select the Socket Type you desire to have for Serial IP communication from the drop-down list.

UDP: If this option is selected, the device will act as a UDP (Connectionless) and listening on the configured Listening IP Port for connection for the client.

TCP Client: If this option is selected, the device will act as a TCP Client and connects to the host processor once the serial port becomes active.

TCP Server: If this option is selected, the device will act as TCP Server and listen on the configured Listening IP Port for connection from the client.

TCP Client/Server 2 Way: If this option is selected, the device will listen on configured Listening IP Port for client connection to communicate with serial device and once the client is disconnected, and the serial device connected to the ttyS1 port needs to report it's status, the device will connect to the host destination to report the device's status.

UDP BroadCaster: If this option is selected, the device will support 5 UDP broadcast addresses.

TCP Client Broadcaster: If this option is selected, the device will support 10 TCP Client broadcast socket using IP Destination configuration for connectivity.

TCP Client Broadcaster Traffic Activator: If this option is selected, the device will support 10 TCP Client broadcast socket using IP Destination configuration for connectivity and would connect only if the serial data is available to broadcast.

Peer IP Address (Required): Enter the peer IP Address into this field. This is required for UDP communication. This specifies the Peer IP address and if set to 0.0.0.0 any remote IP can send UDP packets to our peer port, and return packets will be sent back to the IP of the last host that sent a message. Packets cannot be sent until one is received first (to learn the remote peer's IP). If set to a specific IP, then packets will be sent to this IP only. The recommended setting for this field is "0.0.0.0" to allow any IP to send packets to the peer import number.

Peer IP Port (Required): Enter the peer Port number into the field. This is required for UDP communication. Consult your network administrator for UDP applicaton destination port number.

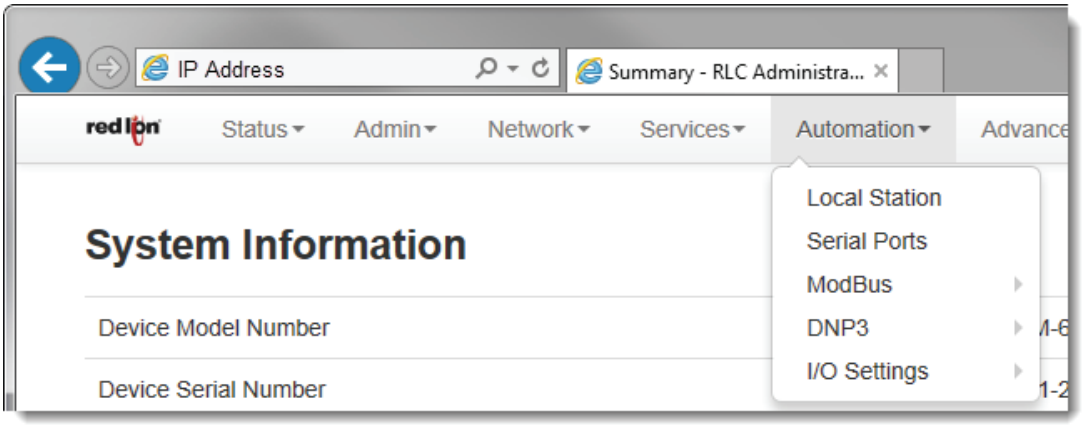
Client IP Port (Required): Enter the client IP port number into this field. This is required if the peer IP Address is set to a specific IP, then packets will be sent to specific IP at this client IP port number only. Consult your network administrator for UDP application destination port number. Set to 0 if the Peer IP is set to "0.0.0.0".

- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

3.6 Automation Tab

The Automation menu contains all aspects of managing your Modbus and DNP3 based I/O.

***Note**: If prompted for an Unlock Key, contact Red Lion Support at support@redlion.net or 1-877-432-9908*



This option is only supported if the IndustrialPro router has been upgraded from an SN prefix to IndustrialPro RAM and for the RAM 9000 series. The IndustrialPro RAM firmware MODBUS application allows it to act as a MODBUS Master acting as an I/O concentrator for MODBUS/DNP3 devices. I/O for these devices can be read or written using MODBUS/DNP3 I/O transfers with the IndustrialPro acting as a MODBUS/DNP3 master. I/O data is stored in a local I/O database.

The IndustrialPro RAM and RAM 9000 series will support:

- I/O transfers using MODBUS/DNP3
- Slave Station Status
- Forwarding of MODBUS/DNP3 messages
- Developing of third party applications using our SDK based on ELDK4.2 and the SIXNET IODB API.

Additionally, the IndustrialPro and RAM 9000 series will act as a MODBUS slave. This allows MODBUS masters to request or update I/O points in the I/O database.

Modbus Configuration:

User interfaces will be provided to configure I/O transfers, the MODBUS forwarding table and serial interfaces. MODBUS configuration data will be stored in an XML based file named modbus.xml. This file will contain the following sections:

- **serials:** xml section to define the parameters used for serial ports for both MODBUS and DNP3.
- **localStation:** xml section to define the local station number and name for both MODBUS and DNP3.
- **remoteStations:** defines remote stations and the I/O transfers associated with them.
- **regAllocation:** defines the number of registers for each I/O type.
- **forwards:** defines the list of remote stations to forward MODBUS requests.

There are two (2) methods to configure these sections.

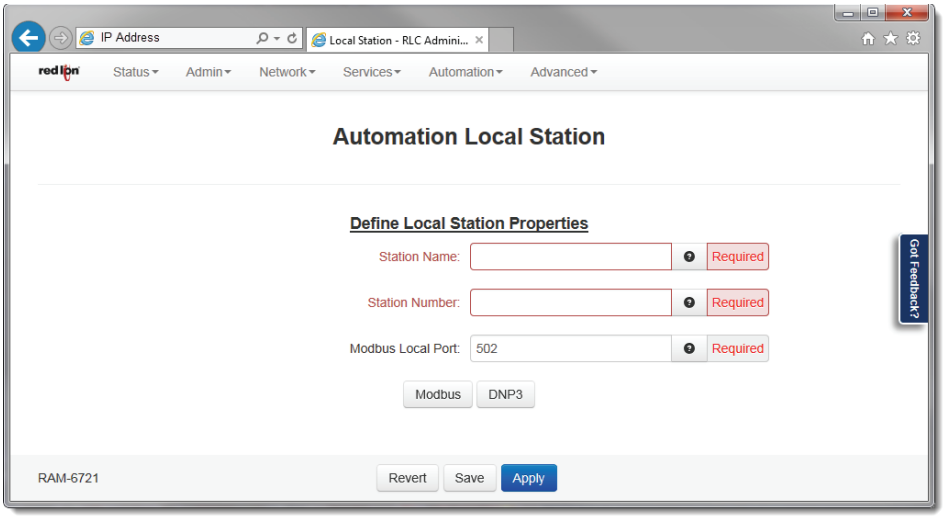
- **CLI:** The command line interface for the cellular modbus gateway (IndustrialPro) provides a Cisco-style telnet command line interface. It writes an XML configuration file, which is used to drive the backend daemons.
- **Web UI:** This method is a WEB based interface which is the focus of this documentation.

The user interfaces will have the ability to:

- Configure/Display local station information such as station name and station number.
- Configure/Display serial ports
- Configure/Display remote stations
- Configure/Display I/O transfers
- Configure/Display MODBUS forward stations
- Configure/Display MODBUS registers allocation

3.6.1 Local Station

- Click on the Local Station sub menu item and the following menu will appear:



Station Name (Required): Enter the name of the local station. The station name must be less than or equal to 32 characters.

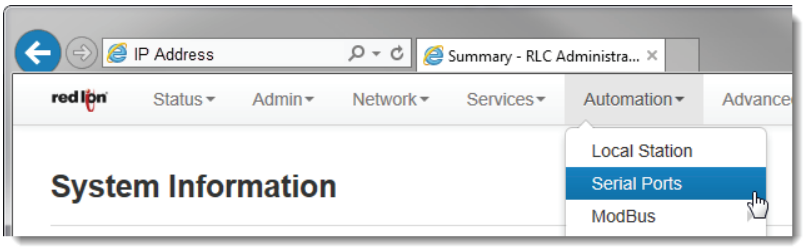
Sation Number (Required): Enter the local station number. The station number must be in a range of 1 - 247.

Modbus Local Port (Required): Enter the local port number. The port must be within the range of 1 - 65535 and the recommended default port is set to 502.

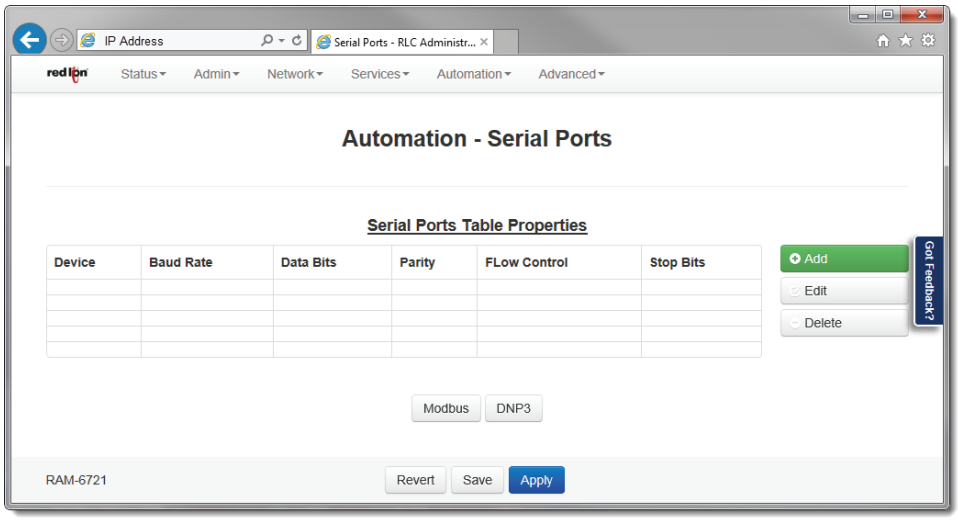
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately.

3.6.2 Serial Ports

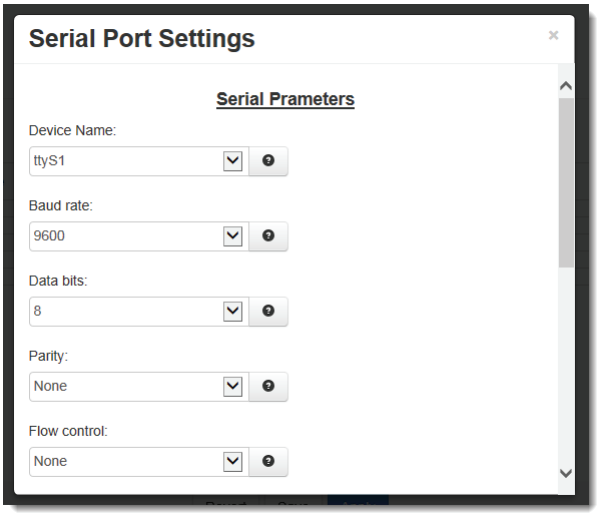
This section is used to configure the RS-232 port that is facing the front of the Red Lion device to integrate into your Modbus/DNP3 schema.



- Click on the “Serial Port” menu item and the following window will appear:



- Click on the Add button and the following pop-up window will appear:



Device Name: Name of the serial device. Valid values: ttys1 (RS232), ttys5 (RS485)

Baud Rate: Baud rate for the serial device. Supported baud rates are: ***300, 600, 1200, 2400, 4800, 9600, 19200*** and ***38400***.

Data Bits: Number of data bits. Supported data bits are ***7*** and ***8***.

Parity: Parity for serial device. Supported parities are: ***none, even, odd, mark*** and ***space***.

Flow Control: Flow control for serial device. Supported flow controls are: ***none, hardware, xon/xoff, half duplex, full duplex.***

Stop Bits: Stop bits for serial device. Supported stop bits are ***1*** and ***2***.

Protocol: Protocol being used on serial device. Supported protocols are: ***DNP3, Modbus Master ASCII, Modbus Master RTU, Modbus Slave ASCII, Modbus Slave RTU, Modbus Master RTU Fwd*** and ***Modbus ASCII Fwd.***

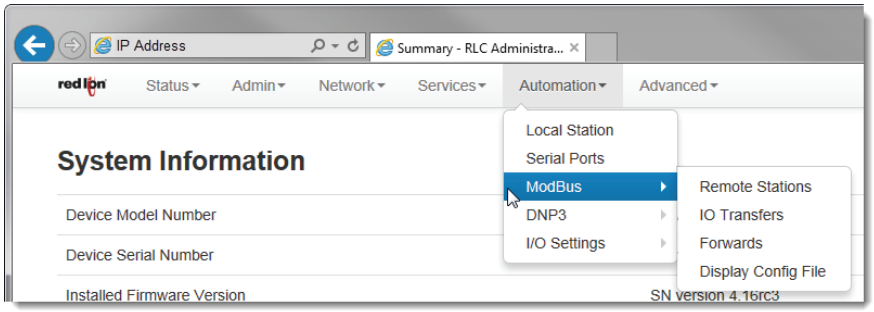
Float Word Order: Controls the swapping of words within floats. Ignored if using Daniel mode. This is needed for configuring the serial slave application. Supported orders are ***LSW*** and ***MSW.***

Long Word Order: Controls the swapping of words within longs. Ignored if using Daniel mode. This is needed for configuring the serial slave application. Supported orders are ***LSW*** and ***MSW***.

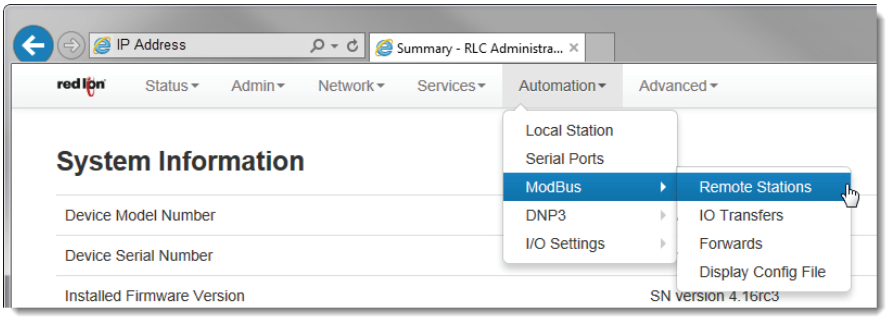
Enable Daniel Mode: Use Daniel mode extensions when dealing with longs and floats. This is needed for configuring the serial slave application.

- Click on the Finish button to populate the Serial Ports Table Properties.
- To delete an address, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

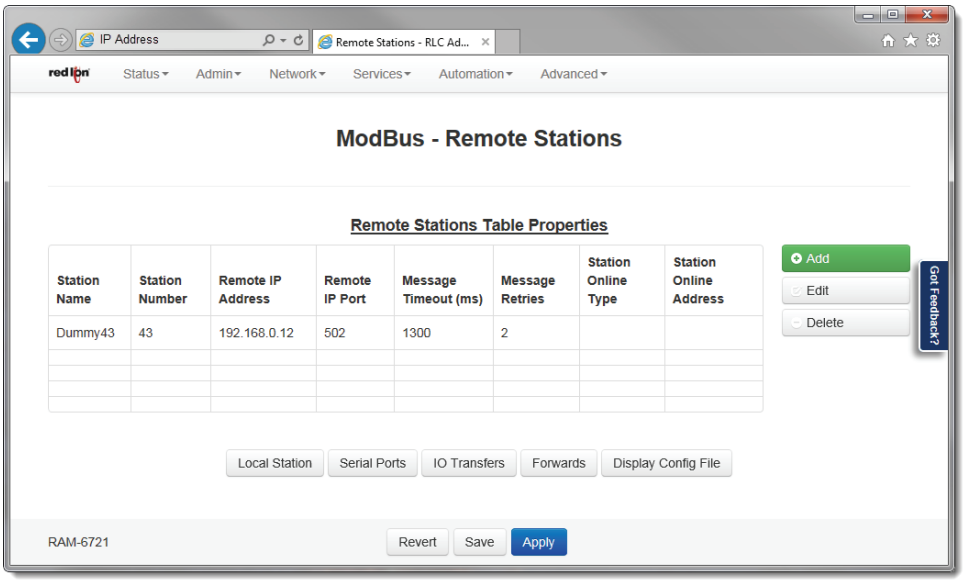
3.6.3 Modbus



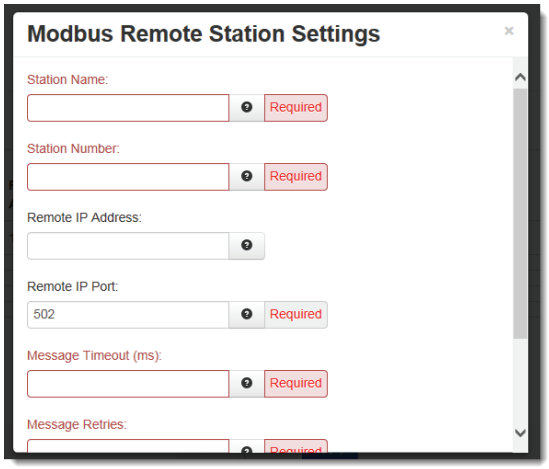
3.6.3.1 Remote Station:



- Click on the Remote Station menu item and the following dialog window will appear:



- Click on the Add button to configure the remote station parameters and the following pop-up window will appear:



Station Name (Required): Enter the name of the remote station. The remote station name must be less than or equal to 32 characters. All the defined remote station names will be populated in the I/O Transfer screens as a selection for assigning I/O transfer for selected remote station name.

Station Number (Required): Enter the remote station number. The station number must be in range of 1-247.

Remote IP Address (Required): Enter the remote station IP address in a valid IPv4 unicast address format, or it may be blank if I/O transfers to this remote station only use the serial port.

Remote IP Port (Required): Enter a valid IP port number (1-65535) that the remote station listens on for MODBUS requests.

Take care to choose a port number not already used by other system services. View *Status->Network->Socket Statuses->TCP* Only for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access (*Network->Firewall->Port Allow/Forwarding Rules->Service Access Rules*).

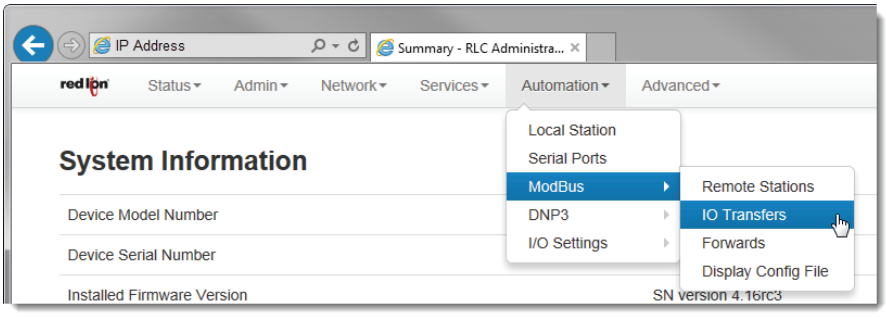
Message Timeout (ms) (Required): Enter the Timeout period, in milliseconds, to wait for an I/O transfer to complete. The valid range is 10ms-60000ms.

Message Retries (Required): Enter the number of times to retry an I/O transfer before giving up. If a station status bit is provided, it would be marked off line when this occurs. The recommended value is 3.

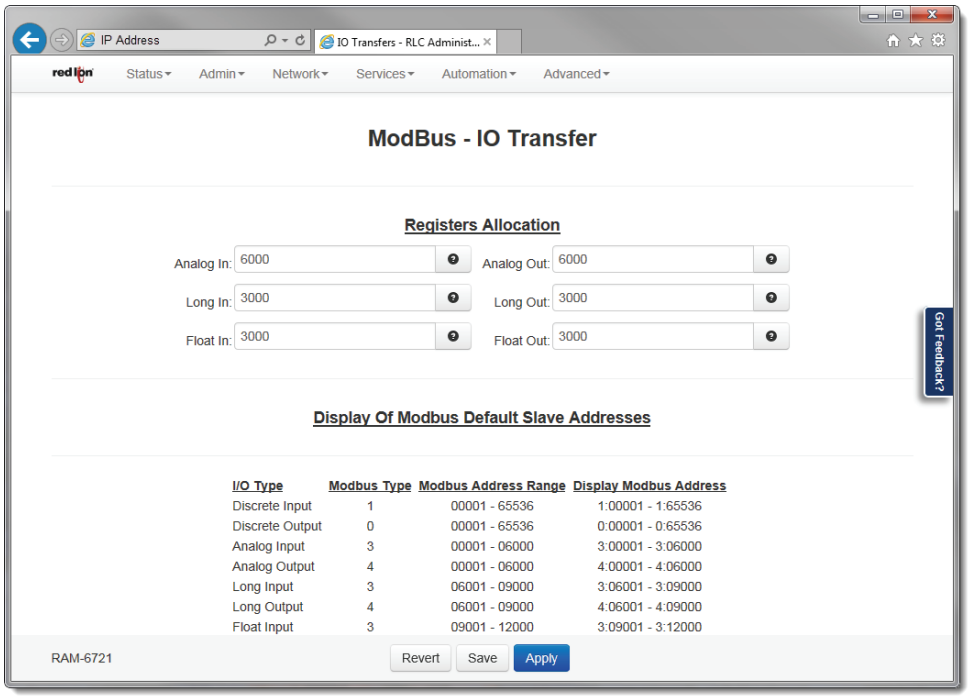
Station Online Address: Discrete input address is used as a station status indicator. If provided, it is set to True when any I/O transfers to a remote station complete successfully, and false otherwise. Enter the Address of a local discrete input or blank if not used.

- Click on the Finish button to populate the Modbus Remote Station Table. If more stations are needed, click on the Add button and enter the required field for each station.
- To edit a Remote Station, select the station in the table and click on the edit button. To delete an existing station, select the station in the table and click on the Delete button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.6.3.2 I/O Transfer



- Click on the I/O Transfer menu item and the following window will appear:


IP Address
IO Transfers - RLC Administ...
Status
Admin
Network
Services
Automation
Advanced
ModBus - IO Transfer
Registers Allocation
Analog In: 6000
Analog Out: 6000
Long In: 3000
Long Out: 3000
Float In: 3000
Float Out: 3000
Got Feedback?
Display Of Modbus Default Slave Addresses
I/O Type | Modbus Type | Modbus Address Range | Display Modbus Address
Discrete Input | 1 | 00001 - 65536 | 1:00001 - 1:65536
Discrete Output | 0 | 00001 - 65536 | 0:00001 - 0:65536
Analog Input | 3 | 00001 - 06000 | 3:00001 - 3:06000
Analog Output | 4 | 00001 - 06000 | 4:00001 - 4:06000
Long Input | 3 | 06001 - 09000 | 3:06001 - 3:09000
Long Output | 4 | 06001 - 09000 | 4:06001 - 4:09000
Float Input | 3 | 09001 - 12000 | 3:09001 - 3:12000
RAM-6721
Revert
Save
Apply

Register Allocation: This section is displaying the default values for the following:

Analog In: By default we support 5000 Analog Input registers, but the range is 1 - 65535.

Analog Out: By default we support 5000 Analog Output registers, but the range is 1 - 65535.

Long In: By default we support 2000 Long Input registers, but the range is 1 - 65535.

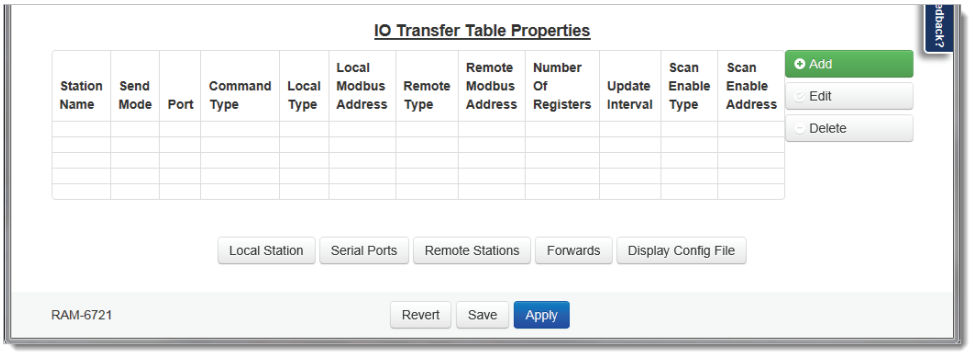
Long Out: By default we support 2000 Long Output registers, but the range is 1 - 65535.

Float In: By default we support 2000 Float Input registers, but the range is 1 - 65535.

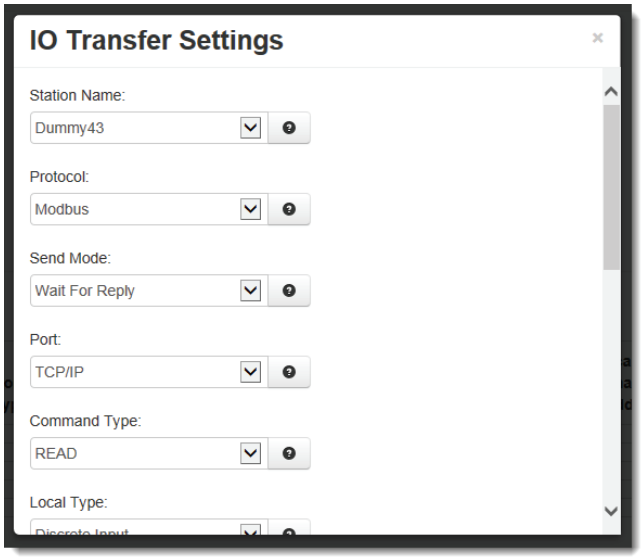
Float Out: By default we support 2000 Float Output registers, but the range is 1 - 65535.

The range of Modbus slave addresses are displayed based on default register allocation. You can change the registers allocation values to your required register values and the range of Modbus slave addresses will be changed based on the new values.

By default, we support 8192 DI registers, 8192 DO registers, 10000 AI registers, 10000 AO registers, 3000 LI registers, 3000 LO registers, 3000 FI registers and 3000 FO registers.



- Click on the Add button to configure the I/O Transfer for the remote station and the following pop-up window will appear:



Station Name: Name of the remote station for this I/O transfer. This option lists the name of all the remote stations that you have already defined and configured in remote station table entry. Select the remote station name that you want for this I/O transfer.

Protocol: Modbus is currently the only supported protocol used for I/O transfers.

Send Mode: Mode used to send an I/O transfer.

> **Wait for Reply:** The MODBUS master must wait for an I/O request that it has sent to complete before sending another request to the remote station.
>
> **Rapid Fire:** The MODBUS master may send many I/O requests to a remote station before waiting for responses from the remote station.
>
> **Valid Values:** Wait for Reply or Rapid Fire

Port: The port that the I/O request is being sent across. The supported ports are **TCP/IP, UDP/IP, ttys1 (RS232) and ttys5 (RS485)**. If UDP/IP or TCP/IP port are used, the remote station selected for this I/O transfer should have its IP address defined.

Command Type: The commands used for I/O transfers are:

READ: Used for reading MODBUS registers from the remote station.

WRITE: Write MODBUS output registers to the remote stations.

WRITE_SINGLE: Write a single MODBUS discrete or analog output register to the remote station. ***Note:*** Only an option when writing a singe discrete output or single analog output.

Local Type: Local Station I/O type. See Table2 - I/O Types and Limits.

Local Relative Address (Required): First address of the local I/O used for the I/O transfer. Valid values are 1 through a value of defined registers configured for specified I/O type. The address ranges are displayed on I/O Transfer screen under 'Display of Modbus Default Slave Addresses' based on configured local register allocation for specified I/O type.

Remote Type: I/O type on the remote station. See Table2, 3, 4 - I/O Types and Limits.

Note: If modbus WRITE operation is selected, this field should be limited to output register types.

Remote Address: First register address for the remote I/O used for the I/O transfer. Valid values are 1 - 65536.

Number of Registers: Number of registers requested in the I/O transfer. This must be 1, if the WRITE_SINGLE command is selected. See Table 2, 3, 4 - I/O Types and Limits.

Note: Number of Registers must be 1, if WRITE_SINGLE command is selected.

Enter Update Interval (ms): Time interval, in milliseconds, for the I/O transfer. The recommended value for this field is 500ms or higher.

Scan Enable Type: I/O Type used for controlling and I/O transfer using either a discrete input or discrete output register. Valid options are **DI** or **DO** or **Blank** if not used.

Scan Enable Address: The address of the discrete register used to control an I/O transfer. Valid values are 0 through number of registers configured for specified I/O type. **Blank** if not used.

- Click on the Finish button to populate the IO Transfer Table Properties. If more stations are needed, click on the Add button and enter the required field for each station.
- To edit a Remote Station, select the station in the table and click on the edit button. To delete an existing station, select the station in the table and click on the Delete button.
- Click on the "Save" button for changes to be saved without activating the interface until you reboot the unit, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

Table 1 - I/O Types and Limits for read commands

I/O Type		Number of regs supported in I/O transfer
Discrete Input	DI	2000
Discrete Output	DO	2000
Analog Input	AI	125
Analog Output	AO	125
Float Input	FI	62
Float Output	FO	62
Long Input	LI	62
Long Output	LO	62

Table 2 - I/O Types and Limits for write commands

I/O Type		Number of regs supported in I/O transfer
Discrete Input	DI	1968
Discrete Output	DO	1968
Analog Input	AI	123
Analog Output	AO	123
Float Input	FI	61
Float Output	FO	61
Long Input	LI	61
Long Output	LO	61

Table 3 - Valid Type Combinations for READ I/O Xfers

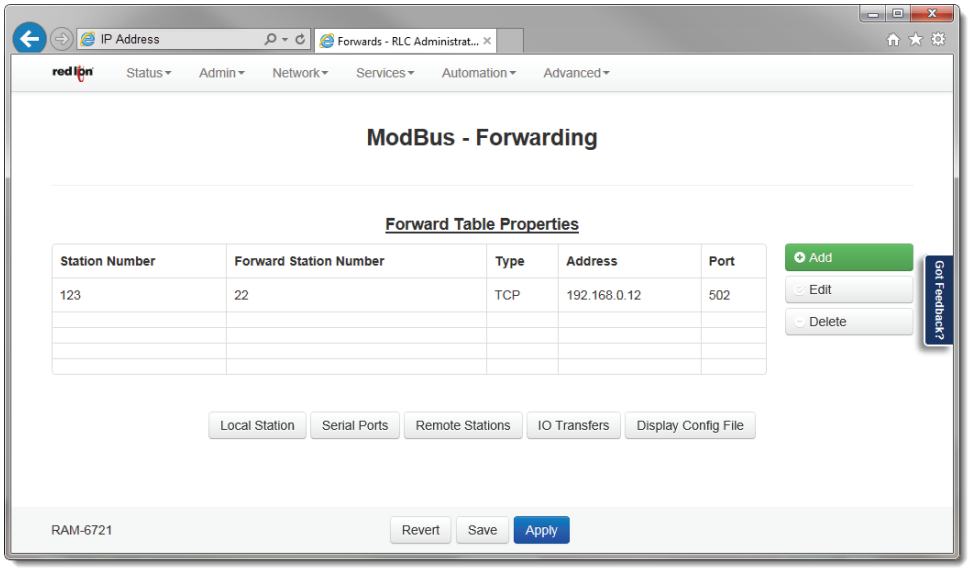
Local Type	Valid Remote Type
DI	DI | DO
DO	DI | DO
AI	AI | AO
AO	AI | AO
FI	FI | FO
FO	FI | FO
LI	LI | LO
LO	LI | LO

Table 4 - Valid Type Combinations for WRITE I/O Xfers

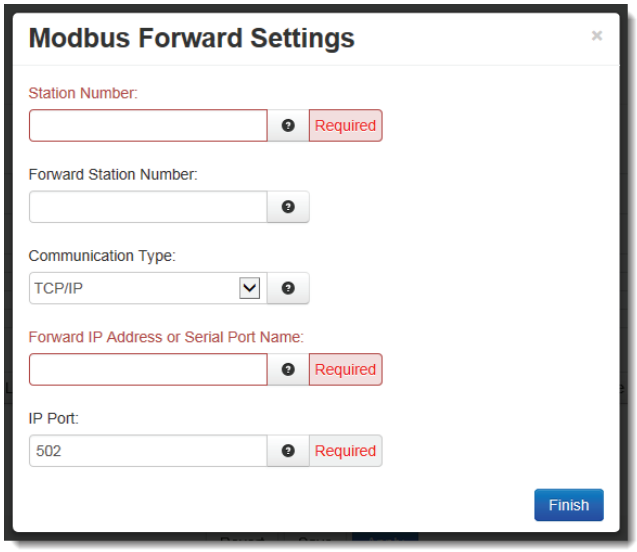
Local Type	Valid Remote Type
DI	DO
DO	DO
AI	AO
AO	AO
FI	FO
FI	FO
LI	LO
LO	LO

3.6.3.3 Forwards

- Click on the Forwarding menu item and the following dialog window will appear:



- Click on the Add button to configure the Forwarding and the following pop-up window will appear:



Station Number (Required): Station number to be forwarded. Valid values are 1 - 247.

Forward Station Number: If supplied, replaces the station number in the request with this value. Valid values are 1 - 247.

Communication Type: Select the forwarding method. Valid options are **TCP/IP**, **UDP/IP** or **Serial** (Serial type can be set in next dialog).

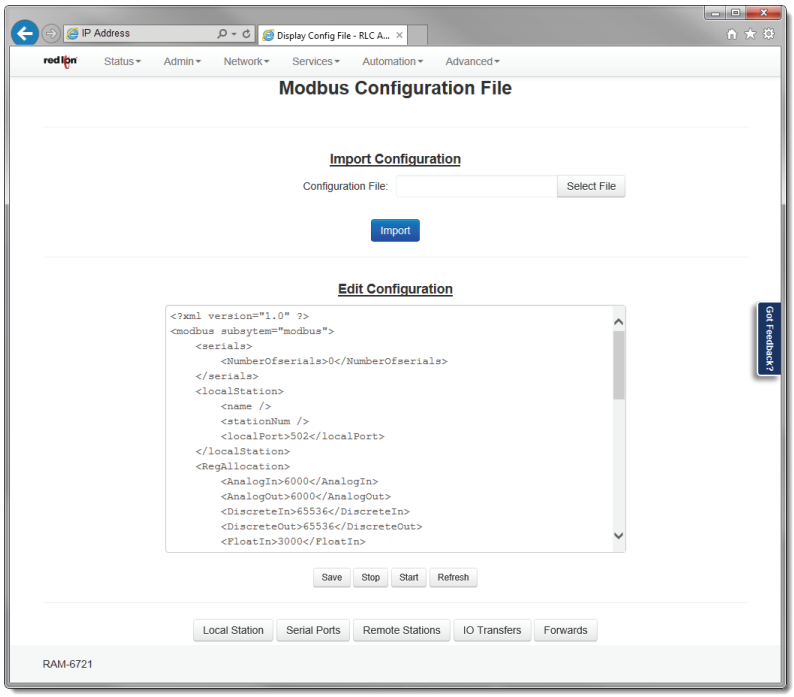
Forward IP Address or Serial Port Name: The address to forward the modbus request if forwarding on with IP, or the serial device name if forwarding the request on the serial port.

IP Port: Enter a valid port number (1-65535) to be used to forward the request to on the remote station. It is recommended that a port number not already used by other system services is chosen. Consult **Status-> Network->Socket Statuses->TCP Only** for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access. (**Network->Firewall->Port Allow/Forwarding Rules->Service Access Rules**).

- Click on the Finish button to populate the Forwarding Table screen. If more than one forward is needed, click and repeat the Add button.
- Click on the “Save” button to save the Forwarding configuration in the modbus.xml file. The “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.6.3.4 Display Config File

- Click on the Display Config File menu item and the following window will appear:



Configuration File: This option will allow you to import a configuration file to replace your existing Modbus configuration file. Click on “Select File” button to select your Modbus.xml configuration file on your PC, then click on the Upload button and once the upload is successful, click on the Import button to replace your existing Modbus.xml configuration file.

Configure Modbus Configuration File: This option will load the Modbus configuration file into the text box for editing. The following controls (buttons) are available:

Save - Save the contents of the text box in to the Modbus configuration file.

Stop - Stop the Modbus service, if it is currently running.

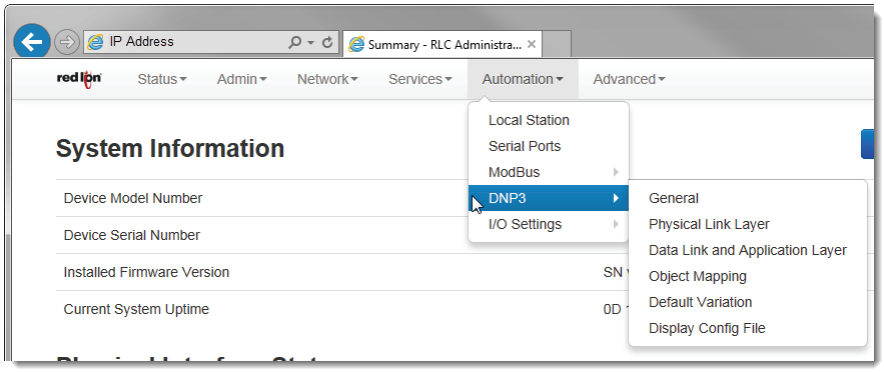
Start - Stop the Modbus service, if it is currently running and start them back up.

Refresh - Reload the Modbus configuration file into the text box.

Download - Download the current Modbus configuration file to your PC as "modbus.xml.txt".

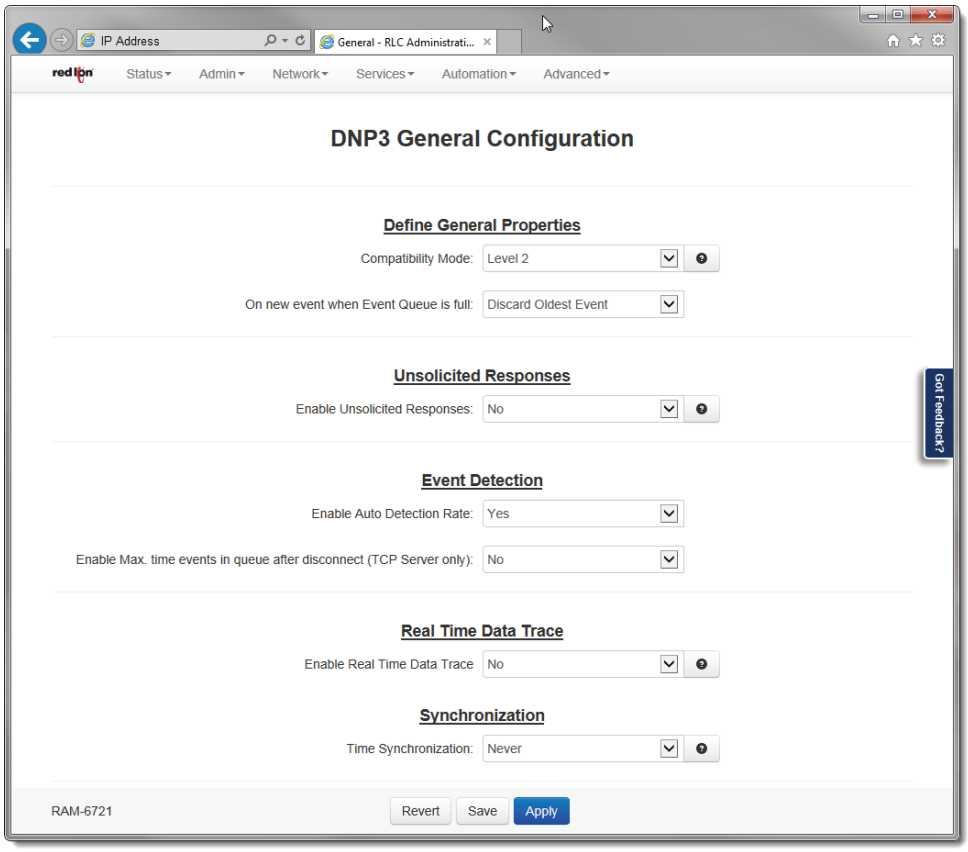
3.6.4 DNP3

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of data acquisition and control equipment.



3.6.4.1 General

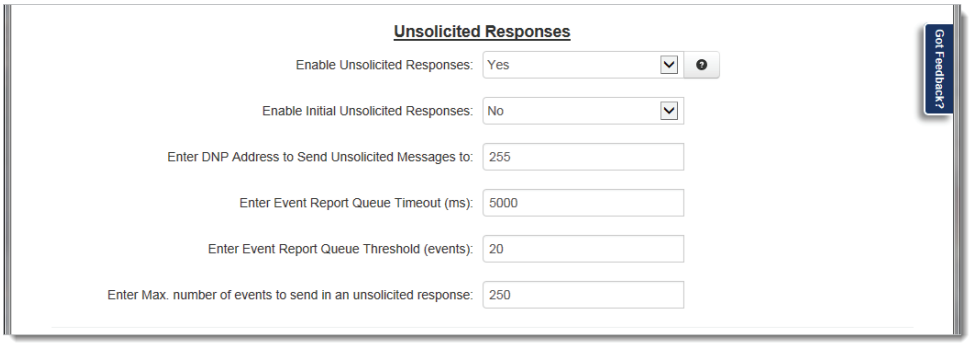
- Click on the DNP3>General menu option and the following screen will appear:



Compatibility Mode: The DNP v3.00 Slave driver can work under two(2) modes: Level 2 or Level 2+.

On new event when Event Queue is full: Select whether to discard the oldest or newest message when log is full.

Enable Unsolicited Responses: Select if the DNP Slave should send unsolicited messages to the DNP Master. If this selection is checked, then the user should also configure the following:



DNP Address to Send Unsolicited Messages to: The address of the station to which DNP Slave will send unsolicited messages in the DNP Address to Send Unsolicited Messages field.

Event Report Queue Timeout (ms): The amount of time in milliseconds any event will be allowed to remain in the event queue before being reported in the Event Report Queue Timeout field. Minimum value: 1,000 ms (1 second), maximum value: 3,600,000 ms (1 hour).

Event Report Queue Threshold (events): The minimum number of events in the event queue required to trigger the generation of an unsolicited even report message in the Event Report Queue Threshold field.

Max. number of events to send in an unsolicited response: The maximum number of events to send in every unsolicited message.

Note: When planning on using unsolicited responses, there must be at least one DNP object configured to generate events on any of the three DNP event classes, or else, no events will be generated and thus no unsolicited responses at all will be generated by the station.

Enable Auto Detection Rate: Check this box to automatically set the detection rate.

Enable Max. time events in queue after disconnect (TCP Server only): Click to enable.

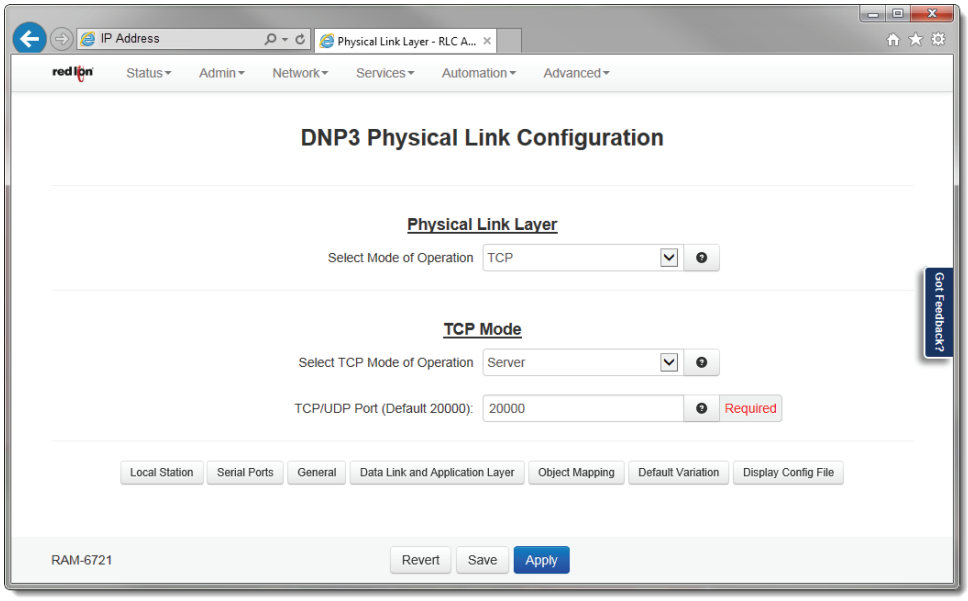
Enable Real Time Data Trace: The DNP V3.00 Slave Driver can be configured to generate real time traces of every Master-Slave DNP V3.00 transaction for diagnosis and debugging purposes. The real time communication data traces can be enabled/disabled at any time from the DNP configuration Add-On and its ASCII output can be redirected either to a text file within the file system for later upload, to a dumb terminal attached to an unassigned serial port of the station, or even to a remote Telnet terminal session over the TCP/IP network by entering the corresponding /dev/ttyp (/dev/ttyp0 to /dev/ttyp3) telnet device.

Time Synchronization: The station can be configured to request Time Synchronization from the DNP V3.00 Master. Requests can be configured to be made at intervals of once per minute, once per hour, once per day or never.

- Click on the “Save” button to save your configuration. The “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

(Navigation buttons across the bottom of the DNP3 screen match the selections made from the drop down tab menu.)

3.6.4.2 Physical Link Layer



Select Mode of Operation: The DNP V3.00 Slave Driver implementation supports RS-232 and RS-485 (two and four wires) over serial port communications as well as TCP/IP and UDP/IP over LAN/WAN communications. When the user selects the Serial Mode, the TCP/UDP section is disabled. The same happens to the Serial section if the Mode of Operation selected is TCP or UDP.

Serial: This section groups all the parameters needed to establish serial communication. When you select this option, the following options will appear in the dialog window:

Serial Port: Select serial port device name from provided drop-down list for serial connection. Options are: ttyS1(RS232) and ttyS5 (RS485).

Enable Collision Avoidance: The DNP V3.00 Slave Driver can be configured to enable or disable collision avoidance. The collision avoidance method implemented is Detection of Transmitted Data with a random pre-transmission back-off time, as recommended by the DNP V3.00 Technical Bulletin 9804-007.

TCP: This section is enabled when the Mode of Operation selected is TCP. The parameters to be configured are:

Select TCP Mode of Operation: DNP slave driver can operate as Server or Client Mode. In Client Mode the user has to set TCP Host field, it is used to enter the name of the Host IP Address.

TCP/UDP Port: Enter the port number where the communication will be established. By default this value is 20,000. This parameter is used in both TCP and UDP protocol.

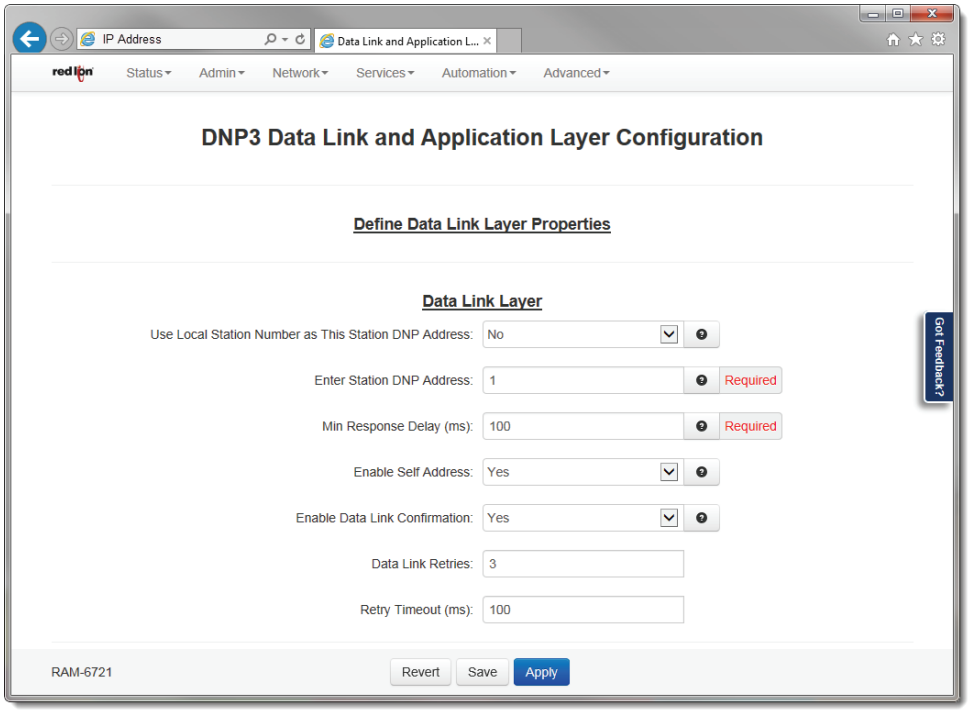
UDP: This section is enabled when the Mode of Operation is set to UDP. The parameters to be configured are:

TCP/UDP Port: Enter the port number where the communication will be established. By default this value is 20,000. This parameter is used in both TCP and UDP protocol.

UDP Host Destination Address to Send Unsolicited Messages: Host Address to which unsolicited messages will be sent when working in UDP mode.

- Click on the “Save” button to save your configuration. The “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.6.4.3 Data Link and Application Layer



Use Local Station Number as This Station DNP Address: DNP address for the slave. This value can be set by the user or automatically assigned by the Add-On. If the check box Same As station Number is selected, then the DNP Address will be equal to the Station Number.

Enter Station DNP Address (Required): Enter the address for this Station if not being automatically assigned.

Min Response Delay (ms) (Required): This is the time delay in milliseconds (from 0 to 65535 msec) before sending the response from the slave.

Enable Self Address: The DNP V3.00 Slave Driver can be configured to send its own DNP Address when a DNP Master asks for it. When this box is checked, if a message is sent with the Self Address (65532) in the destination address field, the will respond with its unique individual address. This feature simplifies the commissioning, troubleshooting and maintenance of devices with an unknown address. If this feature is not enabled, the station will ignore the messages sent to the Self Address.

Enable Data Link Confirmation: The DNP V3.00 Slave Driver can be configured to retry unconfirmed data link primary frames. The number of retries the driver sends and the retry timeout are configurable.

This service is disabled unless Data Link Confirmation option is set to Yes.

Data Link Retries: The number of Retries is configurable between 0 (Data Link Retries disabled) and 255.

Retry Timeout (ms): The Retry Timeout is configurable between 0 (Data Link Retries disabled) and 5000ms

Note: *The Driver's Data Link Layer will attempt to retry (will resend) an unconfirmed data link primary frame when the confirmation has not been received within the configured timeout. If the confirmation fails to arrive after the configured number of retries, the communications link is considered failed and a reset sequence is required before a new primary frame could be sent.*

Enable Application Layer Confirmation: The DNP V3.00 Slave Driver can be configured to retry unconfirmed application link primary frames. The number of retries the driver sends and the retry timeout are configurable. This service is disabled unless Application Link Confirmations check box is selected.

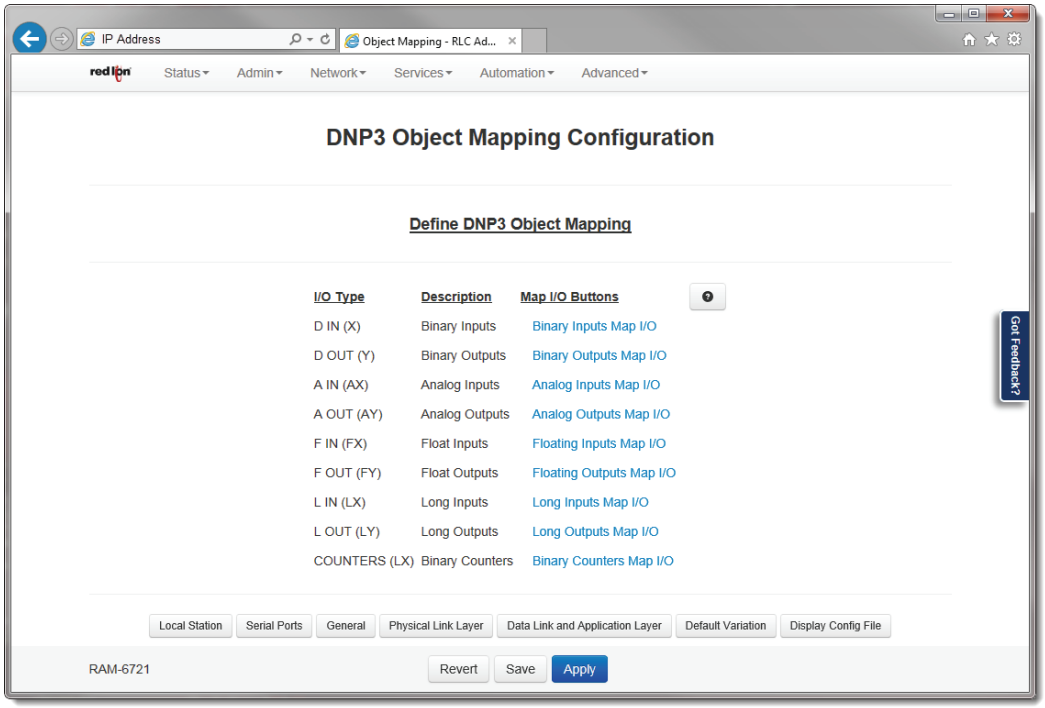
Application Layer Retries: The number of Retries is configurable between 0 (Application Link Retries disabled) and 255.

Application Layer Timeouts (ms): The Retry Timeout is configurable between 0 (Application Link Retries disabled) and 5,000ms

Use different SEQ numbers for CONFIRM and RESPONSE: Check to enable

- Click on the “Save” button to save your configuration. The “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

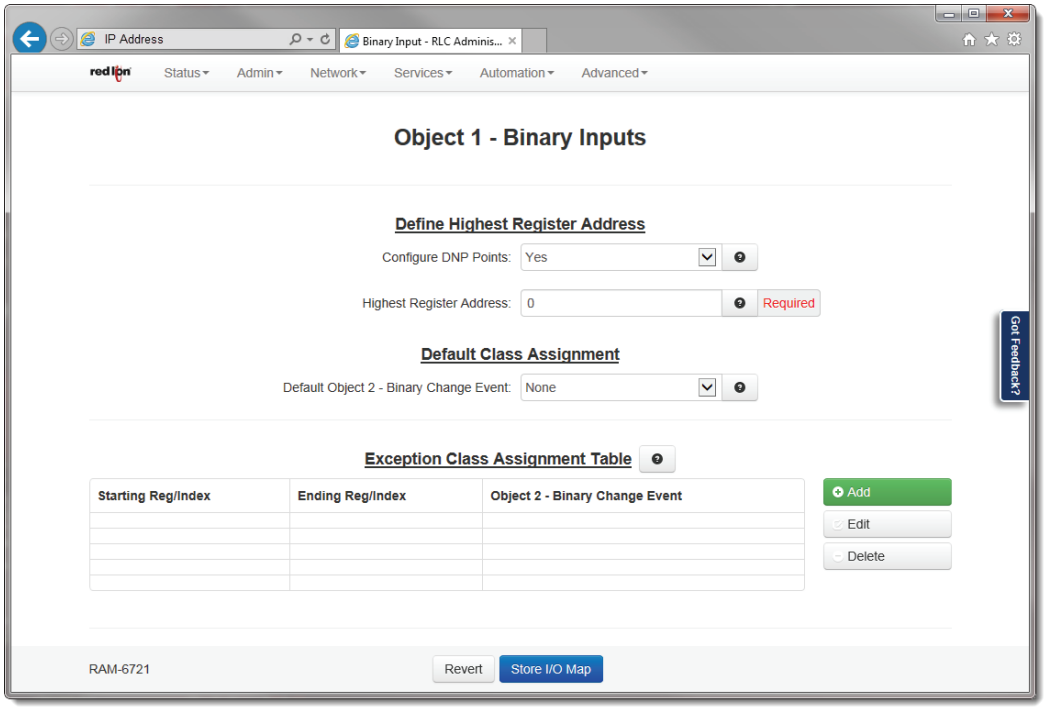
3.6.4.4 Object Mapping



Object Mapping: When clicking on each link a dialog window appears. The dialog window is used to configure and map every DNP point to a specific I/O. ***Note:*** *Each type of I/O must have its corresponding Object Mapping Window opened at least once, or else the I/O won’t be mapped.*

Binary Inputs Map I/O: This section provides configuration of Mapping Binary Input I/O's Reg/Index to DNP points for generating events based on configured Class Assignments when the status of any Binary Input I/O's changes.

Default Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception Class Assignments Table.



Configure DNP Points: If option is No, then no Binary Inputs is mapped as DNP points.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points. If Configure DNP Points option is set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Default Object 2 - Binary Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, 2 or 3), otherwise it should be associated to None. By default all DNP points do not generate events, this feature should be modified by the user.

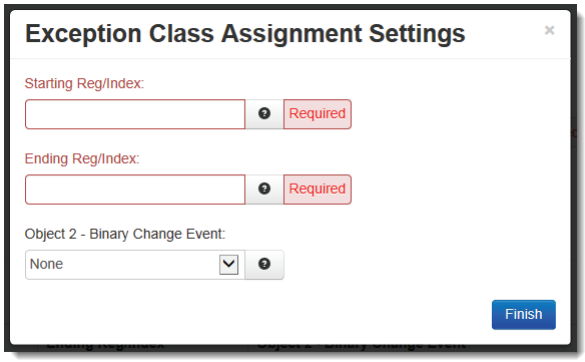
Exception Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured differently than Default Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4, 6-7 are needed to be set for different class assignments than default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception Class Assignments.

Note: The order of table entry ranges must be entered from lowest Reg/Index to highest Reg/Index, otherwise the Web UI will alert the end user for incorrect range entries. The starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address. The maximum suggested entries for the exception table are 10-15 entries.

- Click the Add button to define an Exclusion range.



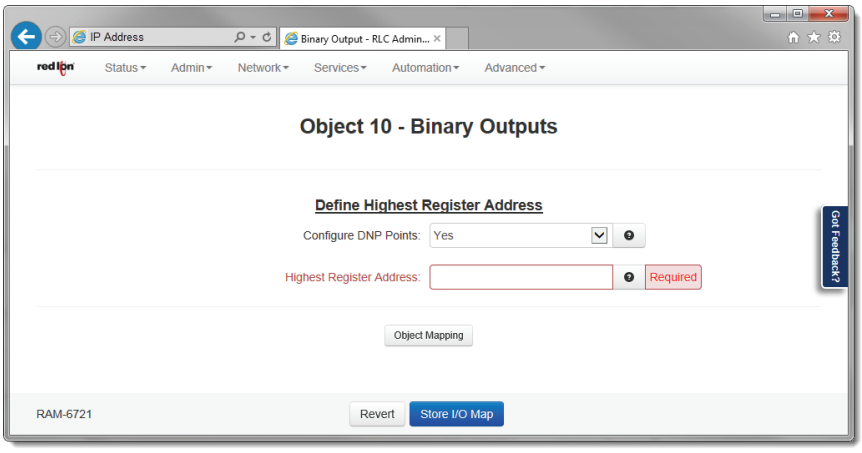
Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Register (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Register.

Object 2 - Binary Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

- Click Finish to enter your exclusion into the table.
- To edit an entry, select the station in the table and click on the edit button. To delete an existing entry, select the station in the table and click on the Delete button.
- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Binary Outputs Map I/O:



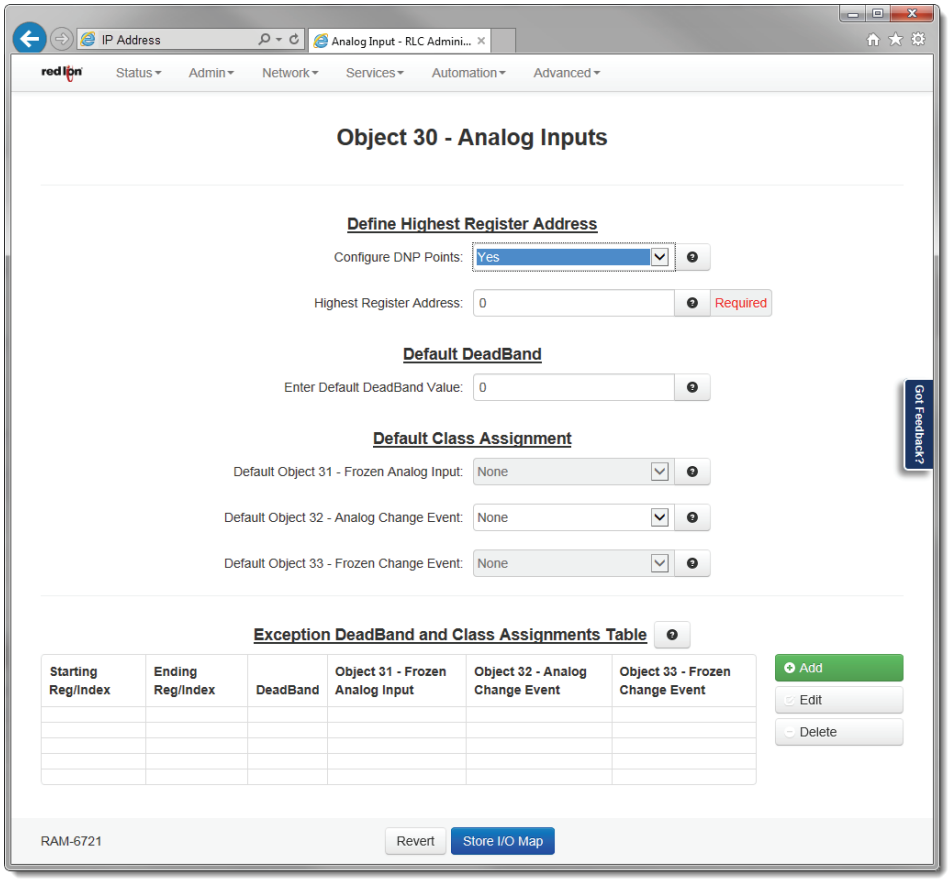
Configure DNP Points: If option is No, then no Binary Outputs are mapped as DNP points.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points. If Configure DNP Points option is set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Analog Inputs Map I/O: This section provides configuration of Mapping Analog Input I/O's Reg/Index to DNP points for generating events based on configured DeadBand and Class Assignments when the status of any Analog Input I/O's changes.

Default DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Configure DNP Points: If option is set to No, then no Analog Inputs are mapped as DNP points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

Enter Default Deadband Value: Values outside this deadband generate events. The deadband parameter sets how even data is generated by your module as a DNP slave device.

For example, the Analog Input deadband being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input Class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Default Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be

associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Default Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Default Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

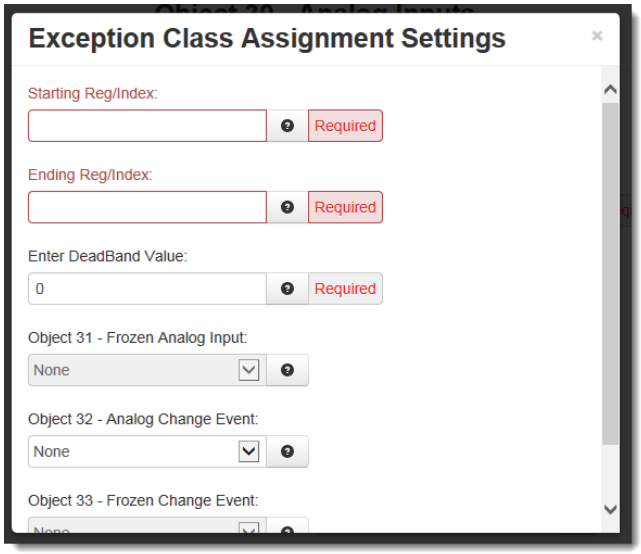
Exception DeadBand and Class Assignments Table: The Exception table provides the ability to define Reg/Index ranges that are needed to be configured differently than Default DeadBand and Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4 6-7 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default DeadBand and Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address.

- Click the Add button and the following dialog window will appear:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Registers.

Enter DeadBand Value (Required): Values outside this deadband generate events. The deadband parameter sets how event data is generated by your modules as a DNP slave device.

For example: The Analog Input deadband being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a

value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

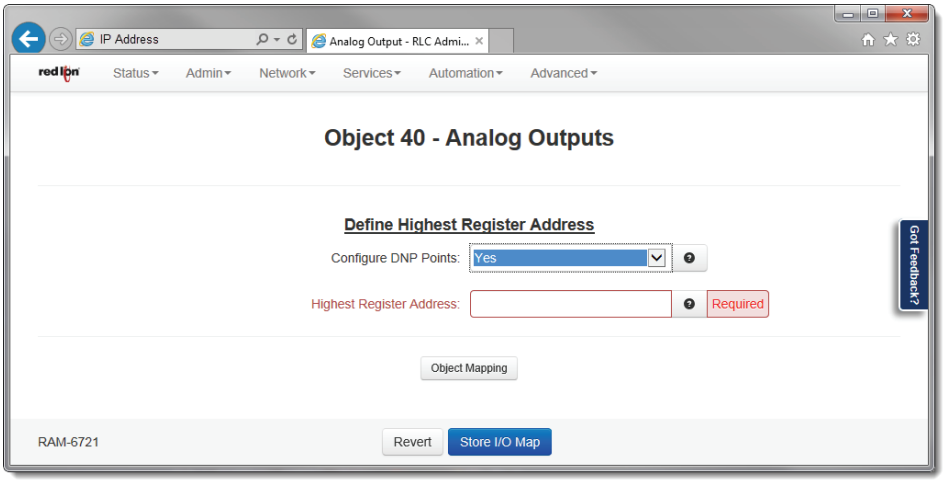
Object 31 - Frozen Analog Input: This field is activated on both levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Object 32 - Analog Change Event: This field is activated on both levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Object 33 - Frozen Change Event: This field is activated on both levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

- Click Finish to enter your exception into the table.
- To edit an entry, select the station in the table and click on the edit button. To delete an existing entry, select the station in the table and click on the Delete button.
- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Analog Outputs Map I/O:



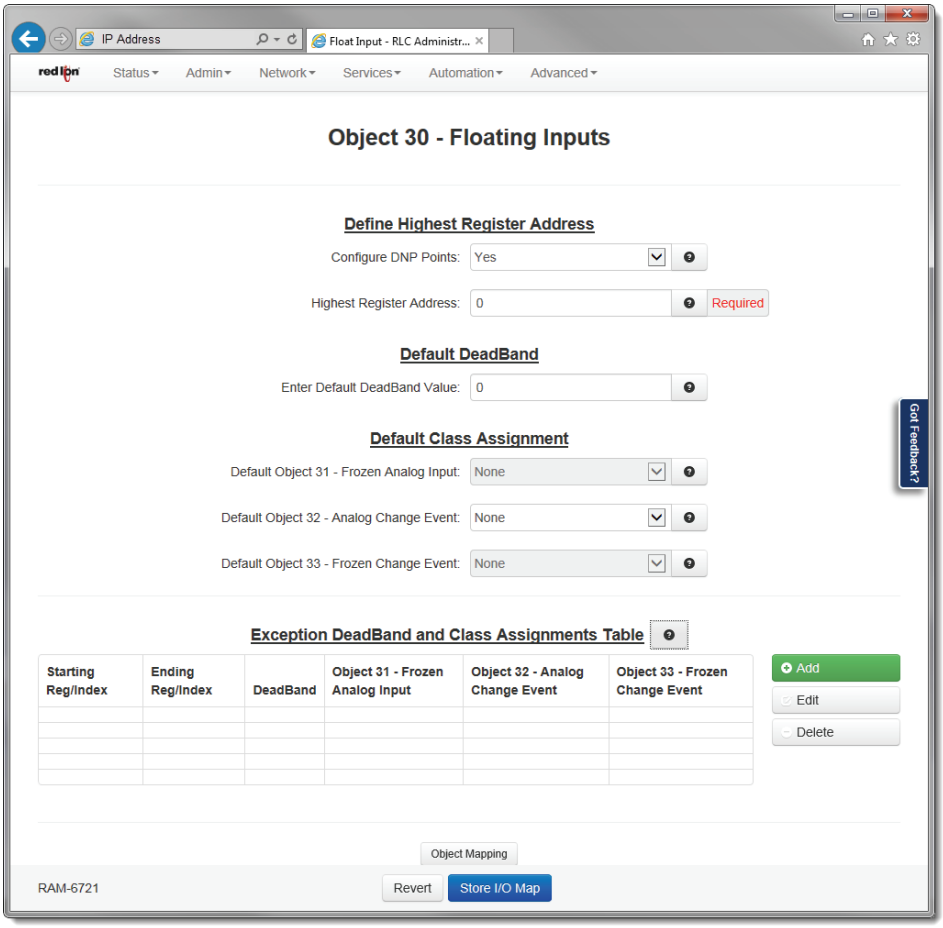
Configure DNP Points: If No is selected, then no Analog Outputs are mapped as DNP points. If set to Yes, the Highest Register Address field is activated.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Floating Inputs Map I/O: This option provides configuration of Mapping Float Input I/O's Reg/Index to DNP points for generating events based on configured DeadBand and Class Assignments when the status of any Float Input I/O's changes.

Default DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Configure DNP Points: If option is set to No, then no Floating Inputs are mapped as DNP points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

Enter Default DeadBand Value: Values outside this deadband generate events. The deadband parameter sets how event data is generated by your module as a DNP slave device.

> For example: The Analog Input deadband being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Default Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Default Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Default Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

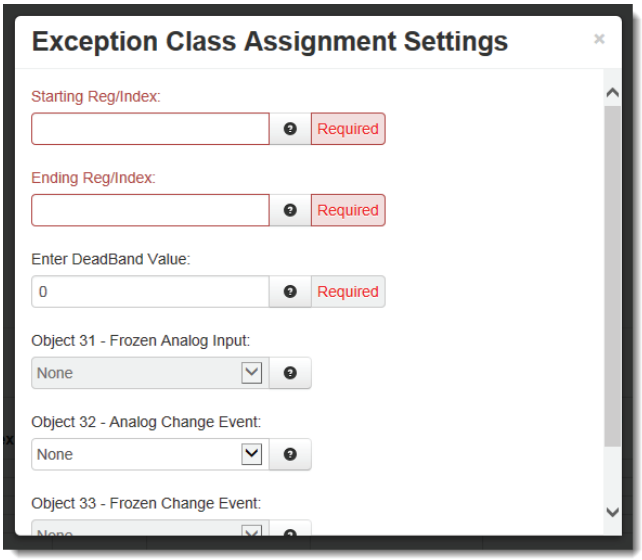
Exception DeadBand and Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured different than Default DeadBand and Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4, 6-7 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default DeadBand and Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address.

- Click the Add button and the following dialog window will appear:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Starting Register.

Enter DeadBand Value (Required): Values outside this DeadBand generate events.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

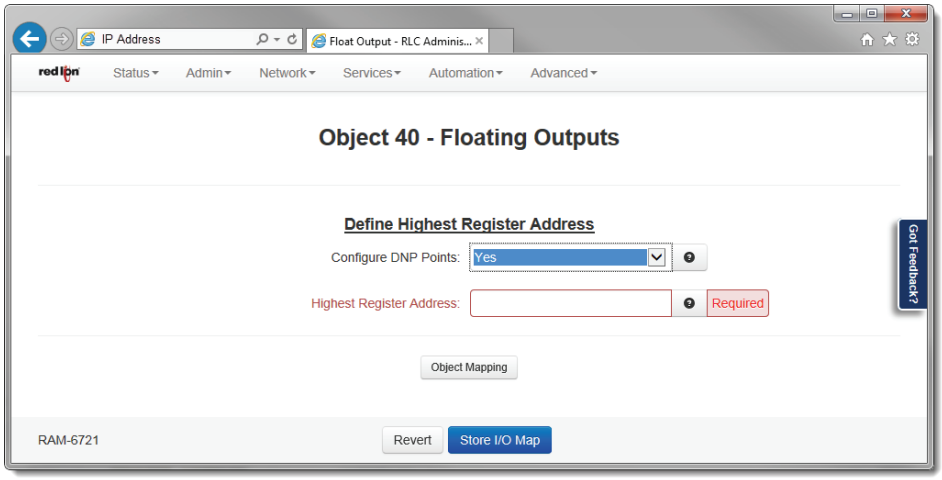
Object 31 - Frozen Analog Input: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Object 32 - Analog Change Event: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

Object 33 - Frozen Change Event: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

- Click Finish to enter your exception into the table.
- To edit an entry, select the station in the table and click on the edit button. To delete an existing entry, select the station in the table and click on the Delete button.
- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Floating Outputs Map I/O:



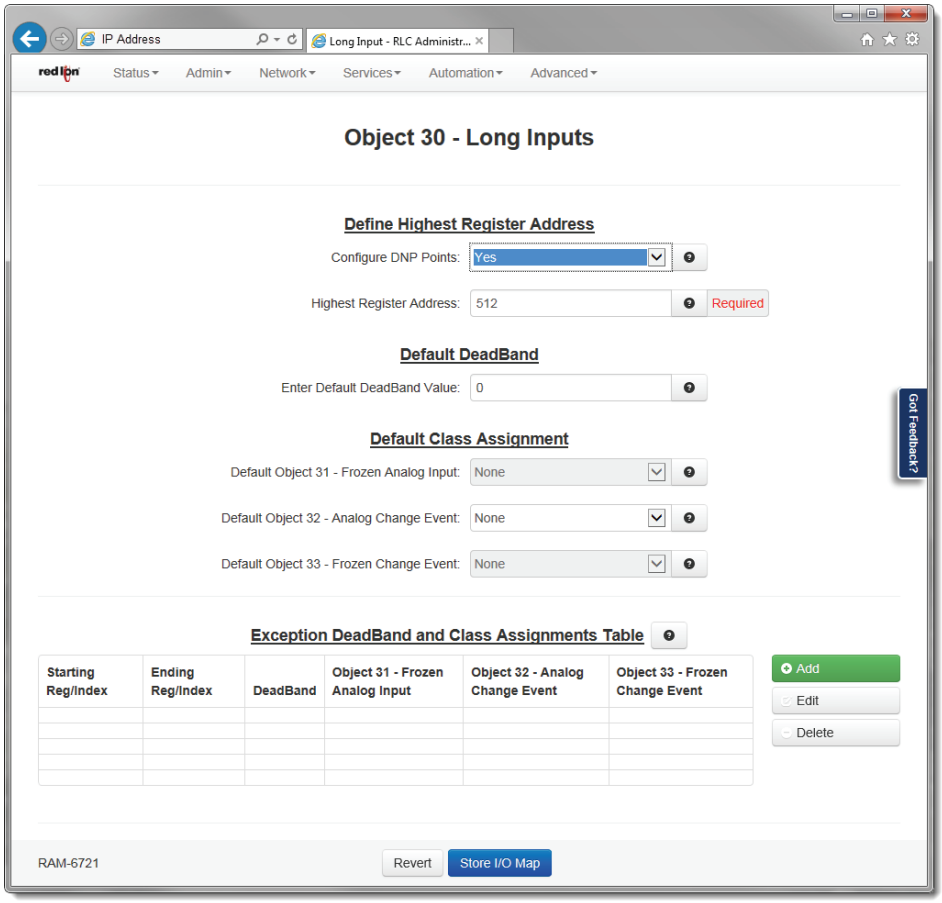
Configure DNP Points: If No is selected, then no Analog Outputs are mapped as DNP points. If set to Yes, the Highest Register Address field is activated.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Long Inputs Map I/O: This option provides configuration of Mapping Long Input I/O's Reg/Index to DNP points for generating events based on configured DeadBand and Class Assignments when the status of any Long Input I/O's changes.

Default DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Configure DNP Points: If set to No, then no Binary Inputs are mapped as DNP points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

Enter Default DeadBand Value: Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP slave device.

> For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the “Analog Input class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Default Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don’t generate events, this feature should be modified by the user.

Default Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don’t generate events, this feature should be modified by the user.

Default Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should

be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

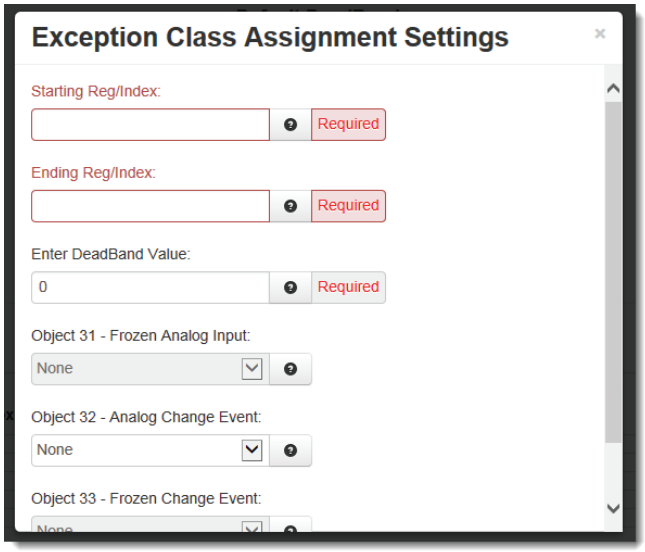
Exception DeadBand and Class Assignments Table: The Exception table provides the ability to define Reg/Index ranges that are needed to be configured differently than Default DeadBand and Class Assignments.

Example: The Stating Reg/Index for Long Input is 512 and if the Highest Register Address is set to 522 and the Reg/Index 514, 516, 518-519 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 512-513, 515, 517 and 520-522 will be set to Default DeadBand and Class Assignments.
- Reg/Index 514, 516 and 518-519 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 514 and 516 in above example has to be the same address.

- Click the Add button and the following dialog window will appear:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Register.

Enter DeadBand Value (Required): Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP slave device.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input DeadBand can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

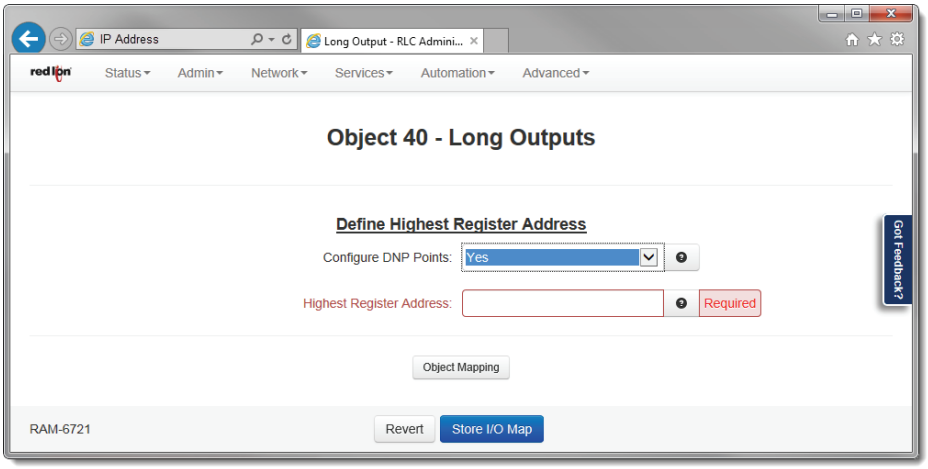
Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't' generate events, this feature should be modified by the user.

Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't' generate events, this feature should be modified by the user.

Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't' generate events, this feature should be modified by the user.

- Click Finish to enter your exception into the table.
- To edit an entry, select the station in the table and click on the edit button. To delete an existing entry, select the station in the table and click on the Delete button.
- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Long Outputs Map I/O:

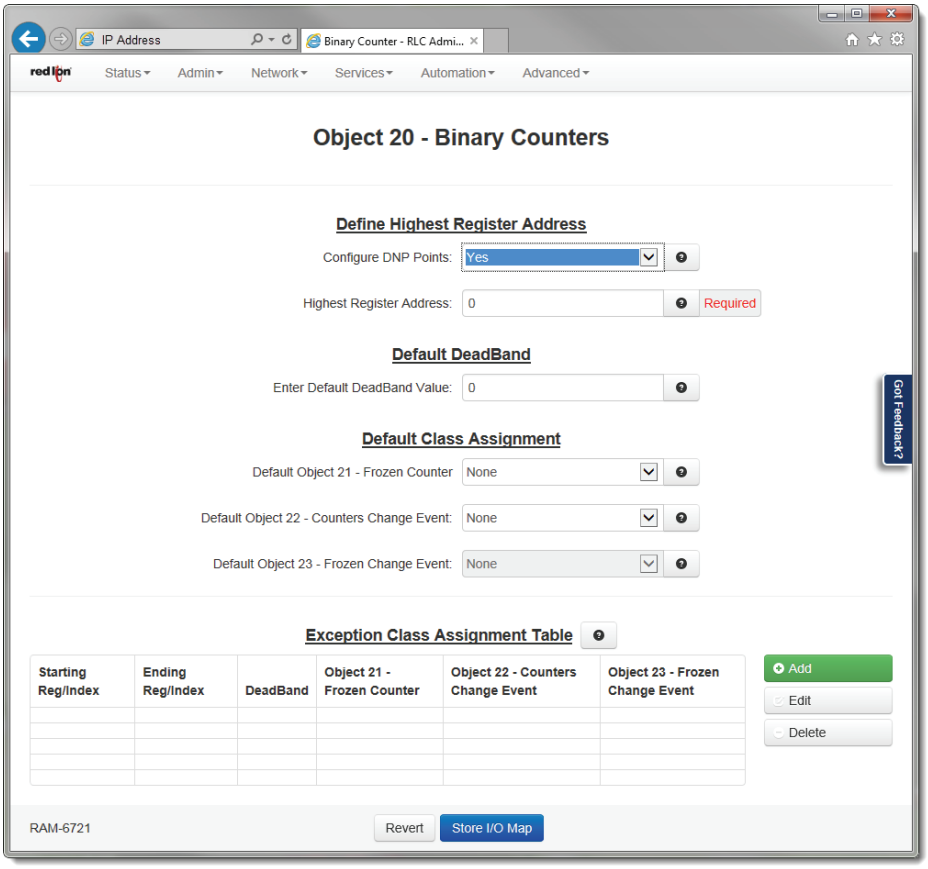


Configure DNP Points: If option is set to No, then no Long Outputs are mapped as DNP points. If set to Yes, the Highest Register Address field is shown ton enter a Highest register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Binary Counters Map I/O: This option provides configuration of Mapping Binary Counters I/O's Reg/Index to DNP points for generating events based on configured DeadBand and Class Assignments when the status of any Binary Counter I/O's changes. DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Configure DNP Points: If option is set to No, then no Binary Counters are mapped as DNP points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP points.

Enter Default DeadBand Value: Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP slave device.

> For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the “Analog Input Class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event

Default Object 21 - Frozen Counter: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don’t generate events, this feature should be modified by the user.

Default Object 22 - Counters Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don’t generate events, this feature should be modified by the user.

Default Object 23 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don’t generate events, this feature should be modified by the user.

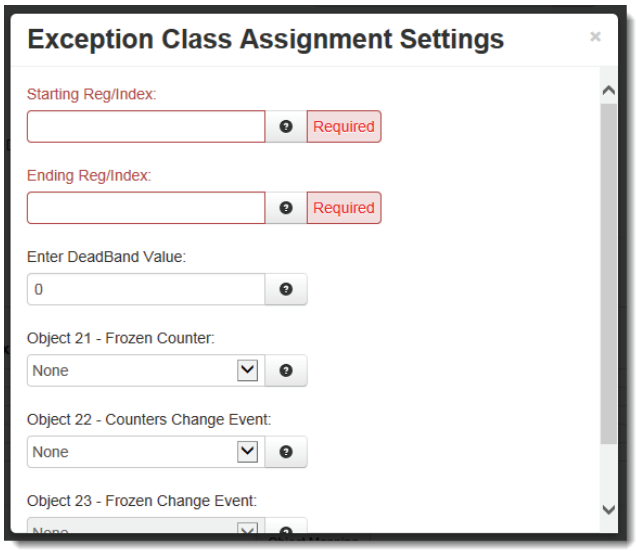
Exception Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured different than Default DeadBand and Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4, 6-7 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default DeadBand and Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address.

- Click the Add button and the following dialog window will appear:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Register.

Enter DeadBand Value: Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP slave device.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being Class 3 data (as set by the “Analog Input Class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input DeadBand can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

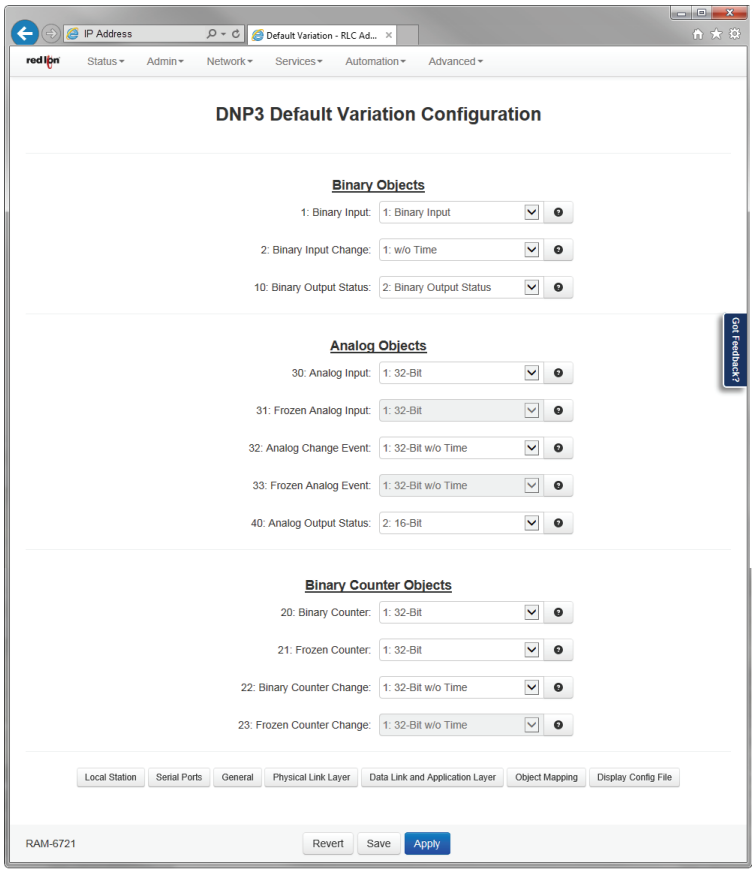
Object 21 - Frozen Counter: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP Points don't generate events, this feature should be modified by the user.

Object 22 - Counters Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP Points don't generate events, this feature should be modified by the user.

Object 23 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP point will generate events. In case a DNP point generates events (Object 2 Binary Change Events) then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP Points don't generate events, this feature should be modified by the user.

- Click Finish to enter your exception into the table.
- To edit an entry, select the station in the table and click on the edit button. To delete an existing entry, select the station in the table and click on the Delete button.
- Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

3.6.4.5 Default Variation



Binary Objects

1: Binary Input: Combo Box that shows the different choices for Object 1 (Binary Input) that the user can select as a default variation.

2: Binary Input Change: Combo Box that shows the different choices for Object 2 (Binary Input Change Events) that the user can select as a default variation.

10: Binary Output Status: Combo Box that shows the different choices for Object 10 (Binary Output) that the user can select as a default variation.

Analog Objects

30: Analog Input: Combo Box that shows the different choices for Object 30 (Analog Input) that the user can select as a default variation.

31: Frozen Analog Input: Combo Box that shows the different choices for Object 31 (Frozen Analog Input) that the user can select as a default variation (only on Level 2+).

32: Analog Change Event: Combo Box that shows the different choices for Object 32 (Analog Input Change Events) that the user can select as a default variation.

33: Frozen Analog Event: Combo Box that shows the different choices for Object 33 (Frozen Analog Input Change Event) that the user can select as a default variation (only on Level 2+).

40: Analog Output Status: Combo Box that shows the different choices for Object 40 (Analog Output) that the user can select as a default variation.

Binary Counter Objects

20: Binary Counter: Combo Box that shows the different choices for Object 20 (Binary Counters) that the user can select as a default variation.

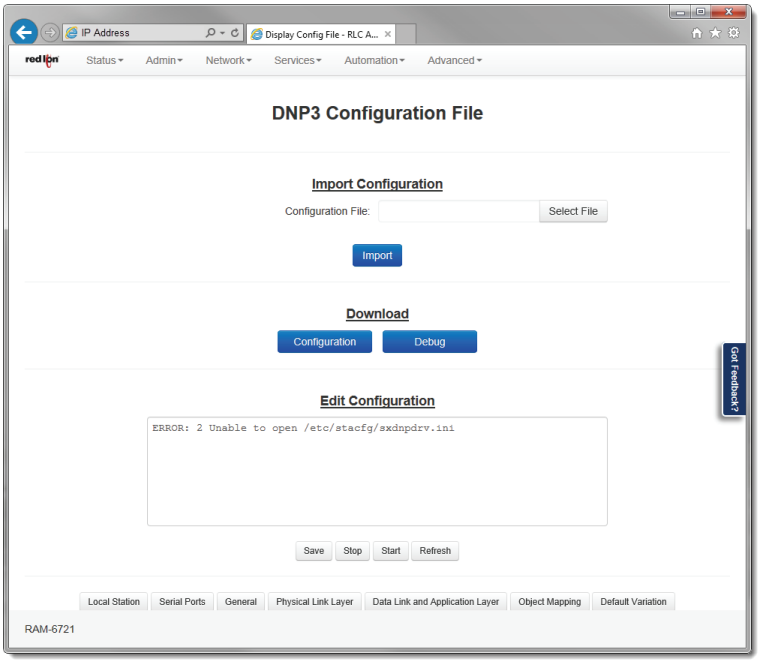
21: Frozen Counter: Combo Box that shows the different choices for Object 21 (Frozen Binary Counters) that the user can select as a default variation.

22: Binary Counter Change: Combo Box that shows the different choices for Object 22 (Binary Counters Change Events) that the user can select as a default variation.

23: Frozen Counter Change: Combo Box that shows the different choices for Object 23 (Frozen Binary Counters Change Event) that the user can select as a default variation (only on Level 2+).

- Click on the “Save” button to save the Forwarding configuration in the modbus.xml file. The “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.6.4.6 Display Config File



From this screen you are able to import, export and manually edit the DNP3 configuration file.

Import Configuration File: This option will allow you to import a configuration file to replace your existing DNP3 configuration file. Simply click on Select File button to select your DNP3 configuration file on your PC, click on the Import button to replace your existing DNP3 configuration file.

Download Appropriate File to your PC: You may use this feature to download the DNP3 configuration file (sxdnp-drv.ini) or DNP3 debug file (dnp3debug.log) to your local drive for review analysis.

Configure DNP3 Configuration File: This option will load the DNP3 configuration file into the text box for manual editing.

The following controls (buttons) are available:

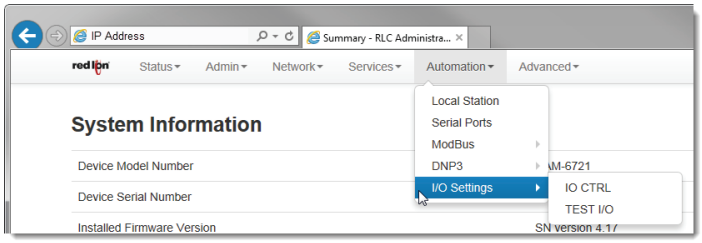
Save: Save the contents of the text box in to the DNP3 configuration file.

Stop: Stop the DNP3 services, if it is currently running.

Start: Stop the DNP3 services, if it is currently running and start them back up.

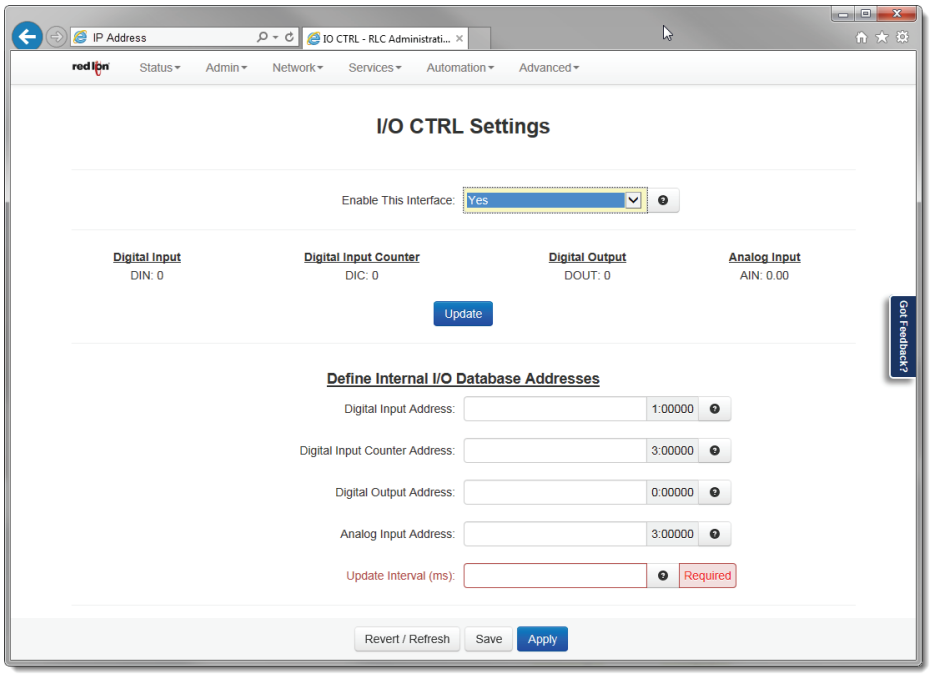
Refresh: Reload the DNP3 configuration file into the text box.

3.6.5 I/O Settings (IndustrialPro and RAM-6000 Series)



3.6.5.1 IO CTRL

- Click on the I/O CTRL menu item and the following window will appear:



Enable this interface: Select Yes to enable the IO/CTRL Interface.

Digital Input Address: Enter the address of internal IODB database for Digital Input I/O control. Valid values for this field are 1 through 65535 as defined for specified I/O type.

Digital Input Counter Address: Enter the address of internal IODB database for Digital Input Counter. The valid values for this field are 1 through a value of defined register allocation configured for Analog Input I/O type. The address ranges are displayed on I/O Transfer screen under 'Display of Modbus Default Slave Addresses' based on configured local register allocation for specified I/O type.

Note: This address cannot be the same address as Analog Input Address. Take care to select a unique address to be used in Analog Input IODB for Digital Input Corner.

Digital Output Address: Enter the address of internal IODB database for Digital Output I/O control. Valid values for this field are 1 through 65535 as defined for specified I/O type.

Analog Input Address: Enter the address of internal IODB database for Analog Input I/O control. Valid values for this field are 1 through value defined registers configured for specified I/O type. The address ranges are displayed on I/O Transfer screen under 'Display Of Modbus Default Slave Addresses' based on configured local register allocation for specified I/O type.

Update Interval (ms) (Required): Enter update interval, in milliseconds, for updating the internal IODB database with value of supported IO/CTRL. The recommended value for this field is 500ms or higher.

Enable Auto update?: Select Yes to enable automatic updating of the I/O ports value. Manual updating is disable while auto update is in effect. The recommended setting for this field is Yes.

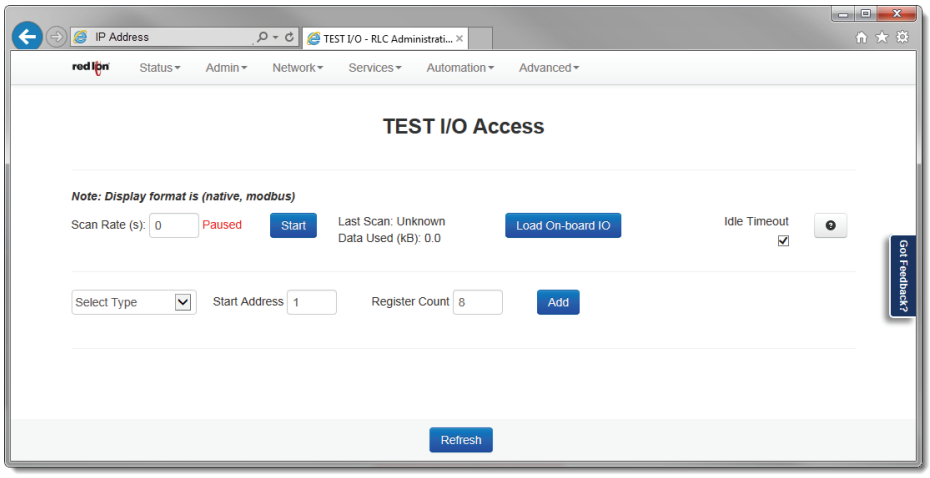
Select update interval: Select the update interval to be used when auto update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 3, 5, 10 or 15.

Be advised that when connected via Cellular interface, the data collected will count towards your total data plan usage.

Click on the "Save" button to save the Forwarding configuration in the modbus.xml file. The "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.6.5.2 Test I/O

Test I/O is used to verify the functionality of I/O states in gateways, RTUs and I/O modules.



The Test I/O interface has been kept simple to make managing the test I/O process easier and keep the screen less cluttered and easier to look at and quickly locate your test values.

Scan Rate: This is the time in which the screen will automatically refresh values from the internal I/ODB.

Idle Timeout: With this enabled (checked), the browser will stop scanning after two minutes of inactivity.

Select Type: From the drop down list, select the type of I/O you would like to test. Valid I/O types are:

Analog In	Discrete In	Long In	Float In
Analog Out	Discrete Out	Long Out	Float Out

Start Address: Once the I/O type has been selected, enter the Start Address.

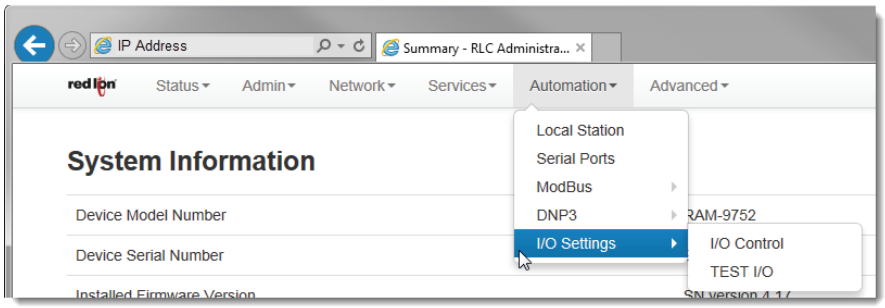
Register Count: Enter the Register Count.

- Click on the Add button to test the I/O.

The messages log shows the range entered and each register that can be edited and monitored for the analog Inputs.

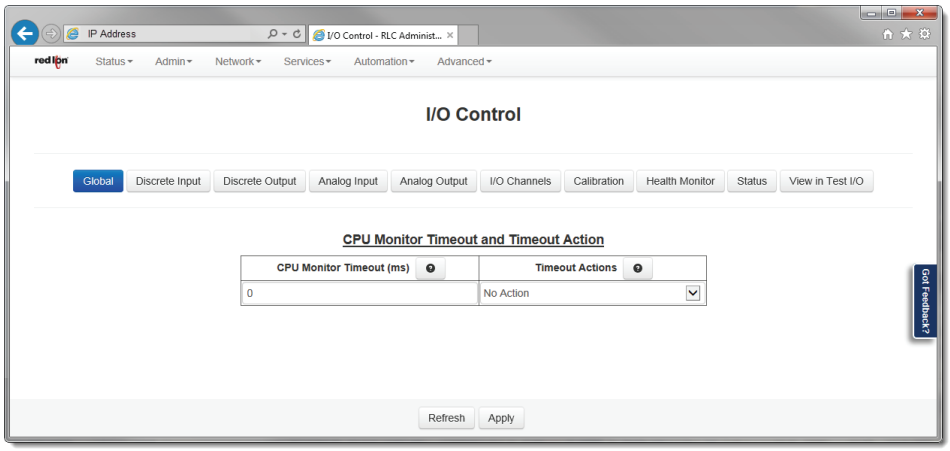
You may enter values here and observe your IODB data from another device / location to see those values get updated, or you may initiate a change from another device/input and observe the changes presented here on your Test I/O interface.

3.6.6 I/O Settings (RAM 9000 Series)

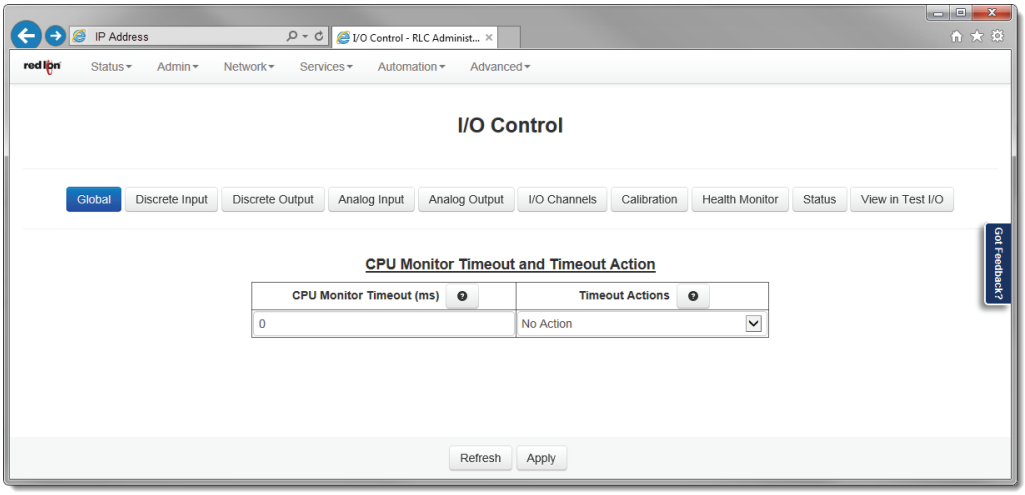


3.6.6.1 I/O Control

- Click on the I/O CTRL menu item and the following window will appear:



Global: Clicking on the Global button will return the user to the main I/O Control dialog window:

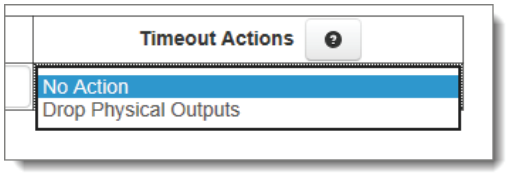


CPU Monitor Timeout (ms): This option is used to make the I/O fail safe if the main CPU stops working. The main CPU controls communication, IODB and code written in C. If the main CPU stops working, the I/O processor will detect that in the time defined in this field. Suggested timeouts are 1000ms to 10000ms. Timeouts faster then 100ms are not recommended. The maximum allowed timeout value is 0xFFFF(65535ms).

Setting this value to 0 will disable the feature. The default valule for this field is 0 (Timeout Disabled).

Select the “Timeout Actions” field to define what the I/O should do when a CPU timeout occurs.

Timeout Actions: When a timeout to the CPU occurs, the selected “Timeout Action” will take effect.



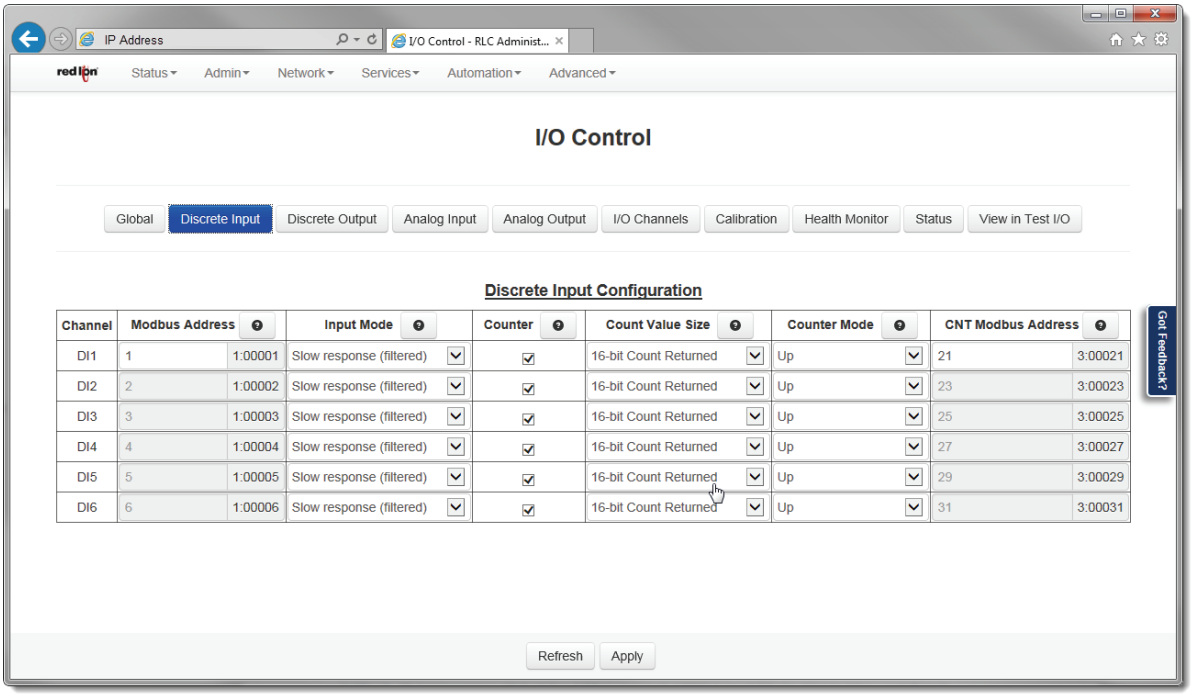
When “Drop Physical Outputs” is selected, all outputs are dropped to and OFF stated.

When “No Action” is selected, outputs will hold their last known value.

In a discrete output module, the OFF state is simply turning the outputs off, in an analog output module, OFF means to set all outputs to a nominal calibrated zero output. TPO Outputs will be set to output 0, but may require the normal TPO interval to elapse before the output will go off.

Discrete Input

- Click on the Discrete Input button and the following dialog window will appear:



Channel: A channel is a physical IO point that can be either analog or digital.

Modbus Address: Configuration must be sequential. Addresses are fixed sequentially from the base address.

Input Mode: This field defines the filtering mode of the Discrete Input channel. Select an option from the drop down list.

> **Disabled**: Selecting this option will completetly disable the channel and a zero (0) will be reported.
>
> **Slow Response (filtered)**: When this option is selected, the Discrete Input will have software filtering applied to the input. Software filtering is suitable when the input is connected to a mechanical switch or relay because wil will eliminate contact bounce. In this mode, counting is limited to a maximum of 10 Hz.
>
> **Fast Response (no filtering):** When this option is selected, the discrete input will have no filtering applied to the input. This option is suitable for solid state switches where no contact bounce is present.

Counter: This option will be available when Input Mode supports counters. When the checkbox is checked, the counter mode is enabled. The Count Value Size, Counter Mode and CNT Starting Address become available and must be configured as well. The counter value is stored in the CNT IODB address.

Count Value Size: This is a plain counter mode that is either 16 or 32-bits in size, which counts on positive edge or negative edge depending on the polarity bit.

> **16-bit Count Returned:** When this option is selected, the count will increment in a single register from 0 to 65535, then roll over to 1 and continue to count upward again.
>
> **32-bit Count Returned**: Select this option to use two (2) consecutive 16-bit registers as one 32-bit register. When the first register rolls over to 1, the second register begins counting at 65536 (second register is most significant) and continues counting upward in 32-bit mode.

Note: Two (2) consecutive registers are always allocated in the “CNT IODB/Modbus Address” column whether set for 16-bit or 32-bit mode. Therefore, when using 16-bit Count Returned option, the second register should be ignored.

Counter Mode: When this option is selected, the counter mode must also be selected. If the 16-bit Counter Returned is selected, the analog input register increases from 0 to 32767, then -32768 to 0. If the 32-bit Count Returned is

selected, the long integer input register increases from 0 to 4.2949673E9, then -4.2949673E9 and back to 0. The menu selections for this options are listed below:

Note: When the Input Mode is set to Slow Response (filtered) some of the Counter Mode options are not particularly suited since the maximum count is 10Hz. For example, Frequency Rate 0.1s would only be capable of measuring one count.

Up: Upward accumulator of input pulses

Run time sec: This is the on-time timer feature that counts the time the associated input is in the ON state. The output for this option is in seconds.

Run time min: This is the on-time timer feature that counts the time the associated input is in the ON state. The output of this option is minutes.

Freq. Rate: Depending on the frequency rate selected, the pulses are accumulated for 100ms, 200ms, 500ms, 1 second, 2 seconds, 5 seconds, 10 seconds, 30 seconds, 60 seconds or 60 minutes.

ON Pulse Width: Width time is ms between consecutive leading (OFF to ON) and trailing (ON to OFF) edges.

OFF Pulse Width: Width time is ms between consecutive leading (ON to OFF) and trailing (OFF to ON) edges.

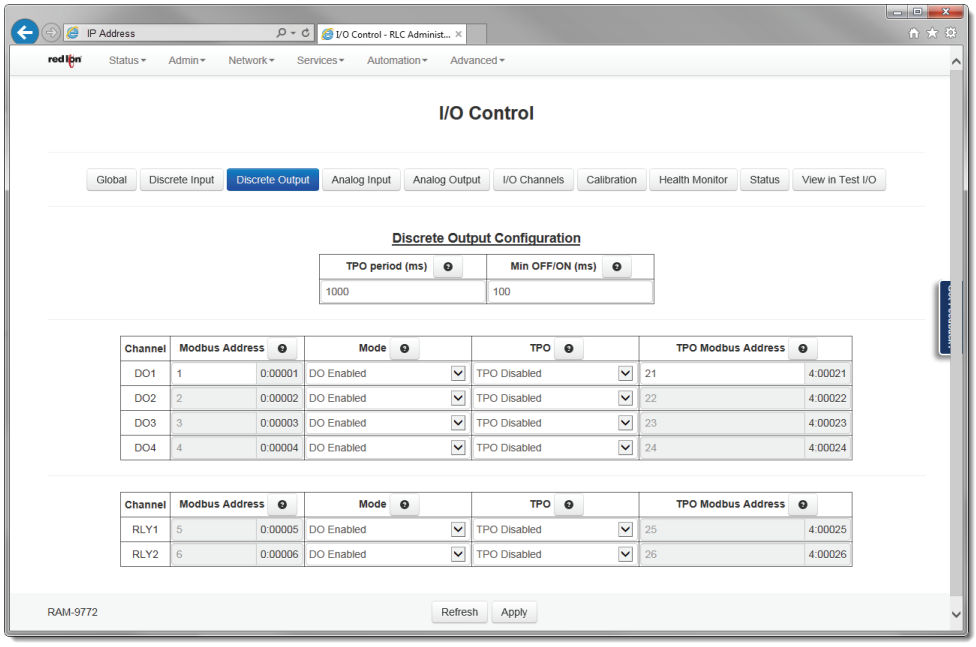
- Pulses longer than the maximum size allowed by the register will result in an overflow condition (full scale 16-bit value equal to 65535)
- Pulses shorter than 1ms will not be accurately detected resulting in erroneous values.
- If no edge is ever detected by an input, the result will read as $0000. Timing only begins when an edge is detected.

Note: Counters are volatile (they will forget their counts if power is lost). Typically, retention of the values and resetting the counts is accomplished in software at the host computer that polls these inputs.

CNT Modbus Address: Configuration must be sequential, CNT addresses are sequential by two registers from the base address.

Discrete Output

- Click on the Discrete Output button and the following dialog window will appear:



TPO period (ms): Time Proportioned Outputs (TPO) are outputs that turn on and off in proportion to an analog value. Typically, the output will turn on and off once during the specified TPO period (cycle time).

Specify a cycle time for all enabled TPO outputs in the module. The range of the cycle time is 20ms to 10 minutes (600,000ms). Each TPO will pulse ON and OFF once during each cycle period, unless a minimum OFF/ON time is specified. The default TPO period value is 1000ms.

Min OFF/ON (ms): Specify a minimum OFF/ON time (shortest allowable ON or OFF pulse) if the output devices are not capable of changing stat withing 1⁄32767 of the desired time. (Mechanical relays are an example of such a device).

The range for the minimum OFF/ON time is 10ms to 10 minutes. All settings will maintain the time proportion by waiting multiple cycle times, if needed, to turn an output ON or OFF. The default value for this field is 100ms.

Channel: A channel is a physical IO point that can be either analog or digital.

Modbus Address: Configuration must be sequential. Addresses are fixed sequentially from the base address.

Mode: This option will enable/disable the discrete output channel.

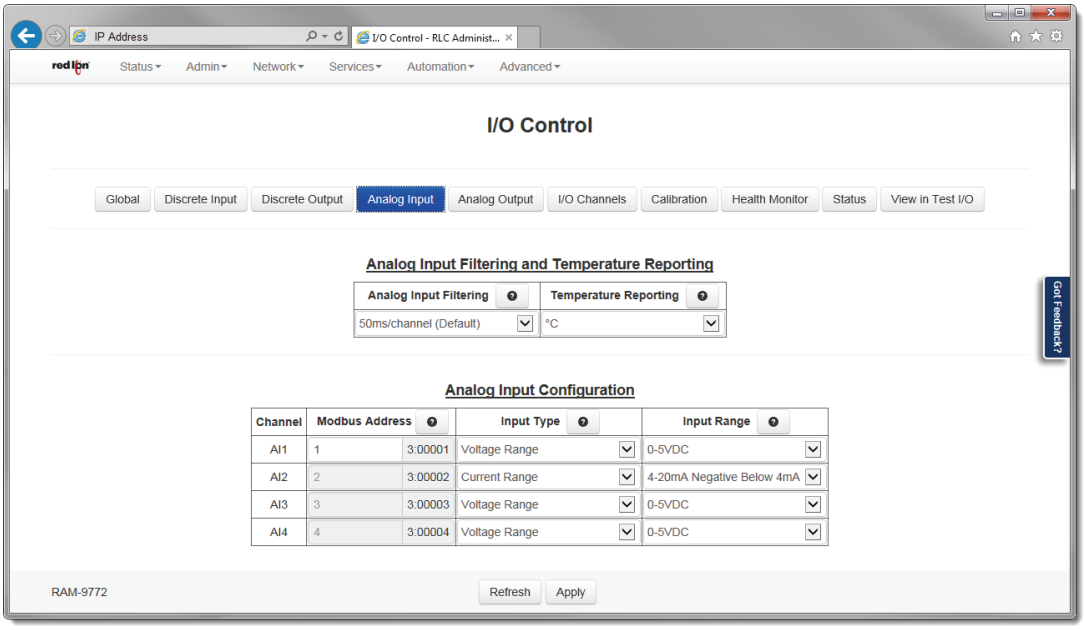
TPO: Select the Enable Time Proportioned Outputs (TPO Disabled/Enabled) in the dropdown list, if it is desirable to have any discrete outputs in this module function as time proportioned outputs. All discrete ouputs support this TPO capability. Each channel can function as a TPO output or a discrete output, but not both. If TPO is enabled, the TPO period, Min. OFF/ON and TPO IODB/Modbus address must be configured as well.

The analog value associated with each channel will control how long the TPO will be ON or OFF (16-bit value from 0-32767). For example, an analog value of zero will tell the output to be OFF. A value of 3276 (10% of 32767) will turn the output on for 10%of the “TPO Period” value. 32767 (full scale) will control the output to be ON at all times except for Min OFF/ON time.

TPO Modbus Address: This field indicates the register addresses of the analog outputs that control the TPO’s when enabled. Configuration must be sequential. Addresses are fixed sequentially from the base address.

Analog Input

- Click on the Analog Input button and the following dialog window will appear:



Analog Input Filtering: The table below explains the filtering (integration) options on the analog inputs. The faster the integration time, the quicker the channels will be sampled. Howerver, quicker samples will render less accurate readings. For most accurate readings, select the slower sample/filtering settings.

Integration Time	Samples/Second (1 Channel)	Notes
3ms/channel	320	Best for high speed reporting and lower accuracy
6ms/channel	160	
12.5ms/channel	80	
25ms/channel	40	
50ms/channel (default)	20	Best for 50/60Hz noise rejection and higher accuracy.
100ms/channel	10	
200ms/channel	5	

Temperature Reporting: Choose from 1°C, 0.1°C, 1°F and 0.1°F. When set for 1°C or F, the temperature is reported as whole degrees and if set for 0.1°C or F, the reported value is the temperature multiplied by 10 and reported as an integer.

Channel: A channel is a physical IO point that can be either analog or digital.

Modbus Address: This field indicate the register addresses for each channel. Configuration must be sequential. Addresses are fixed sequentially from the base address.

Input Type: Select the type of signal that will be connected to the input.

Disabled: This option will completely disable the channel so the channel will always report a zero. The Input Range is configuration will be disabled as well.

Voltage Range: When this option is selected, the analog input will be configured to take a DC voltage range. The Input Range must also be configured.

Current Range: With this option selected, the analog input will be configured to take current instrumentation input (0-40mA or 4-20mA). The Input Range must also be configured.

Input Range: Select the range that will be connecte to the input channel.

0-5 VDC and 0-10 VDC: This option will be available when the Voltage Range option is selected. In these modes, the value will be scaled from the selected range (0-5 VDC and 0-10 VDC) to 0-32767 (decimal).

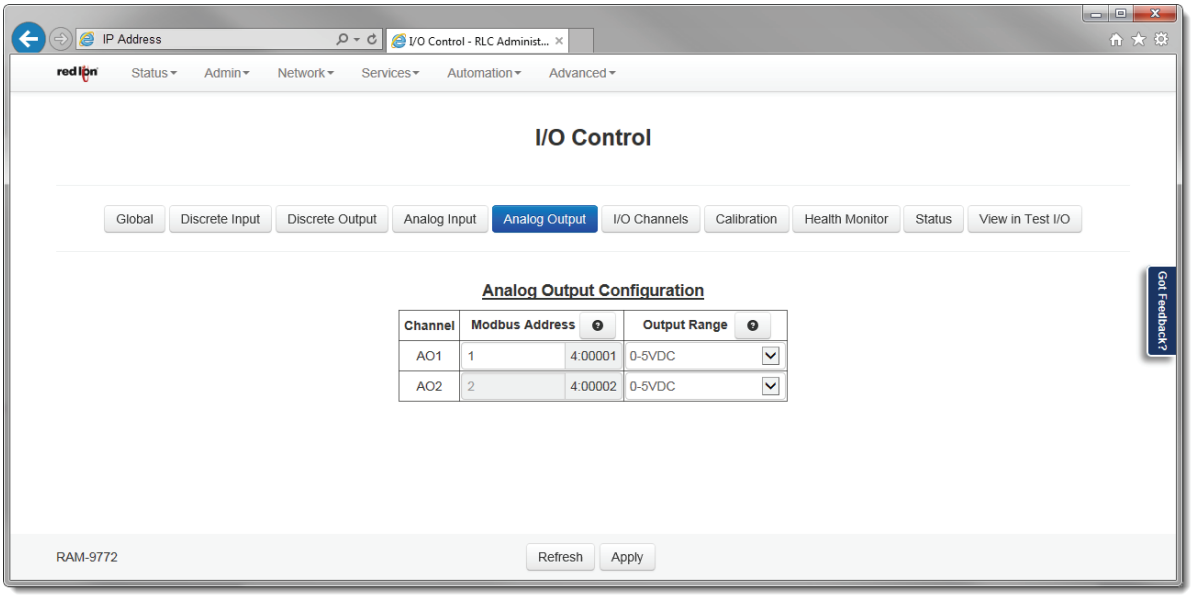
0-20 mA Positive Results Only and 4-20 mA Positive Results Only: These options will be available when the Current Range option is selected In thse modes, the value will be scaled from the selected range (0-20mA and 4-20mA) to 0-32767 (decimal). No negative results will be displayed. If no signal is connected, the analog input vlaue reported will be 0 (decimal).

4-20 mA Negative below 4mA: When this option is selected, the 4-20 mA range will be scaled from 0-32767 (decimal). A negative value will be displayed when nothing is connected to the input or the instrument is no longer supplying a current. This setting can be used to detect a failed or disconnected instrument.

Note: Negative numbers are determined by using the most significant bit in the 16-bit decimal value as a signed bit. When the most significant bit is 0, the value is positive. When the most significant bit is 1, the value is negative. Therefore, the value read from the channel may be displayed differently depending on the device that is reading that value. For example, negative values may also be read as any decimal value above 32767.

Analog Output

- Click on the Analog Output button and the following dialog window will appear:



Channel: A channel is a physical IO point that can be either analog or digital.

Modbus Address: This field indicate the register addresses for each channel. Configuration must be sequential. Addresses are fixed sequentially from the base adddress.

Output Range: Select the type of signal to be supplied by the output channels.

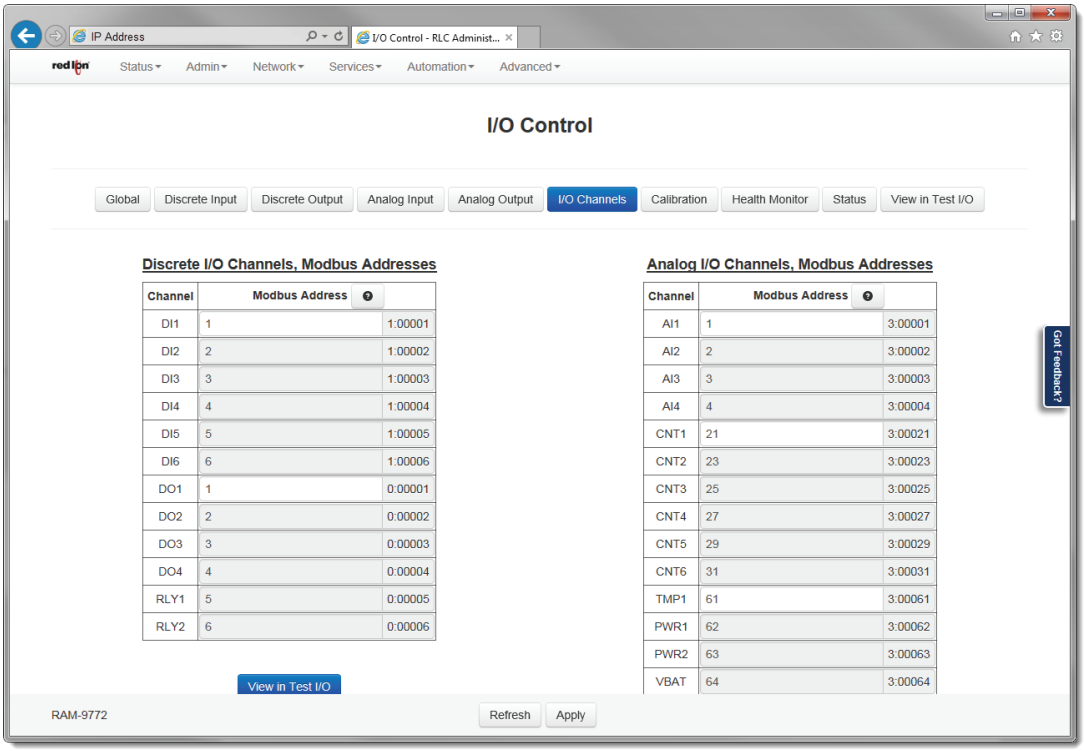
Disabled: This option will completely disable the output channel.

0-5 VDC: When selected, the analog output will be configured to supply a DC voltage from 0-5 VDC. The ouput voltage will be scaled to 0-32767 (decimal value in the IODB/Modbus Address field).

0-20 mA: When selected, the analog output will be configured to supply a current from 4-20 mA. The output voltage will be scaled to 0-32767 (decimal value in the IODB/Modbus Address field).

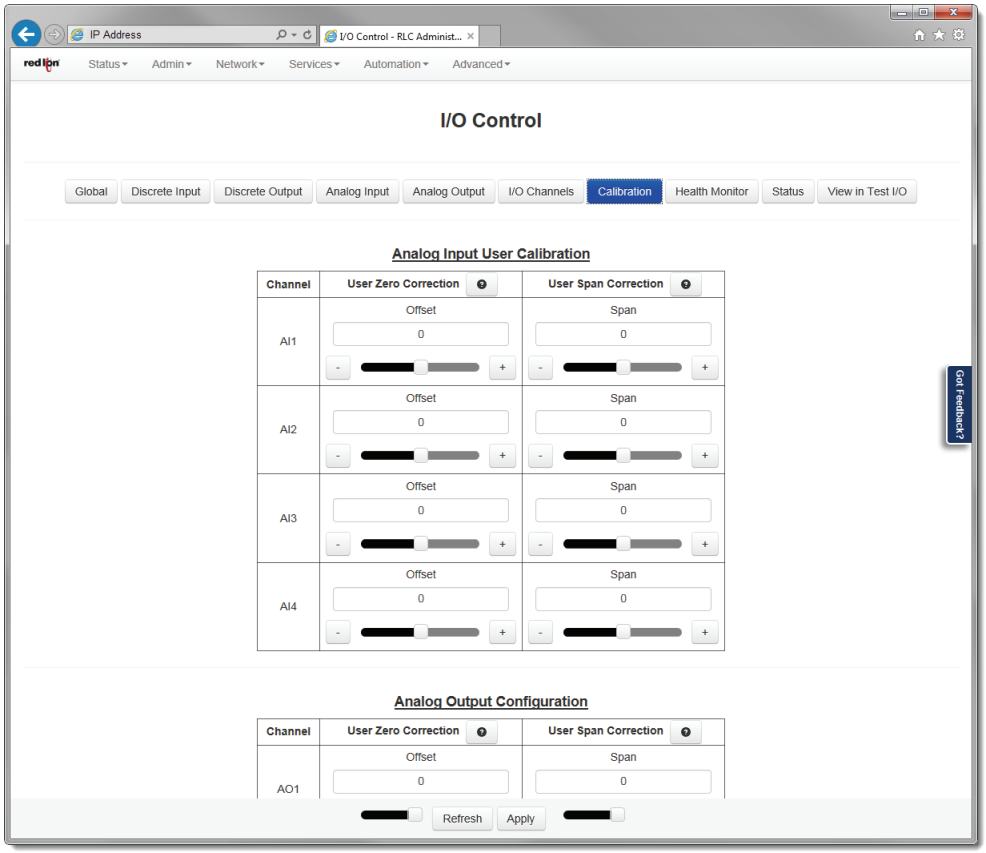
I/O Channels

- Click on the I/O Channels button and the dialog window below will appear. The I/O Channels dialog window will provide a list of all the channels with their associated IODB/Modbus Address.



Calibration

- Click on the Calibration button and the following dialog window will appear:



Channel:Channel: A channel is a physical IO point that can be either analog or digital.

User Zero Correction: Manually adjust the user offset calibration for analog inputs/outputs. Every analog/input is calibrated at the factory according to the specified accuracy. The user calibration is supplied to account to adjust the reported values to account for wiring or instrumentation errors. For this reason, most inputs/outputs will NOT need to be calibrated.

Zero or Offset calibrations are used to adjust the reported value from 5 to 15% full scale. The calibration can be adjusted coarsely by moving the slide bar from left to right with a mouse. For fine adjustments, use the -/+ buttons on either side of the slide bar. The corresponding adjustment will be displayed in the calibration configuration. The calibration will not take effect until the apply button is clicked.

A negative adjustment (negative calibration value) will cause the reported channel value to go down. A positive adjustment (positive calibration value) will cause the reported channel value to go up. The larger the calibration value the greater the difference will be between the reported channel value and the actual measured value.

Instructions on adding user calibrations:

Use this method to calibrate a channel using the manual slide bar user calibration.

1. Set your analog signal device for a near minimum (5 to 15% full scale) output. Measure the device's output at the module's screw terminals with a precision meter or external standard monitor.
2. Apply the small signal to the analog input channel. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the Offset value by the using the slide bar and arrows in the Offset display box. Click the Apply button and observe the effect of the new offset factor. Repeat this step until a satisfactory reading is obtained.
3. Set your analog device for a near full scale (85 to 95% full scale) output. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the span value by using the slide bar and arrows in the span display box. Click the Apply button and observe the effect of the new span factor. Repeat this step unit a satisfactory reading is obtained.
4. The channel is now calibrated.

User Span Correction: Manually adjust the user span calibration for analog inputs/outputs. Every analog input/output is calibrated at the factory according to specified accuracy. The user calibration is supplied to account to adjust the reported values to account for wiring or instrumentation errors. For this reason, most inputs/outputs will NOT need to be calibrated. Span calibration are used to adjust the reported value from 85 to 95% of full-scale.

The calibration can be adjusted coarsely by moving the slide bar to the left or right with a mouse. For fine adjustments, use the -/+ buttons on either side of the slide bar. The corresponding adjustment will be displayed in the calibration configuration. The calibration will not take effect until the apply button is clicked. A negative adjustment (negative calibration value) will cause the reported channel value to go down. A positive adjustment (positive calibration value) will cause the reported channel value to go up. The larger the calibration value, the greater the difference will be between the reported channel value and the actual measured value.

Instructions on adding user calibration:

Use this method to calibrate a channel using the manual slide bar user calibration:

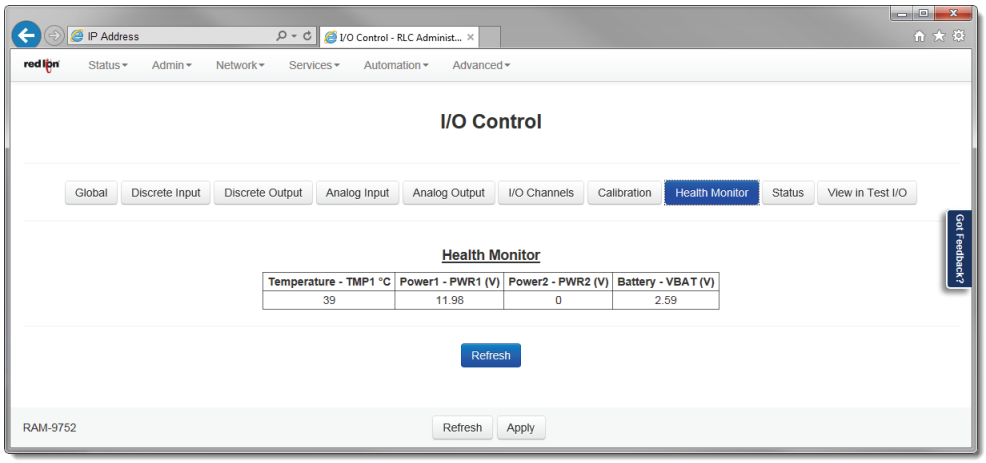
1. Set your analog signal device for a near minimum (5 to 15% full scale) output. Measure the device's output at the module's screw terminals with a precision meter or external standard monitor.
2. Apply the small signal to the analog input channel. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the Offset value by using the slide bar and arrows in the Offset display box. Click the Apply button and observe the effect of the new offset factor. Repeat this step until a satisfactory reading is obtained.
3. Set your analog signal device for a near full scale (85 to 95% full scale) output. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the Span value by using the slide bar and arrows in the

Span display box. Click the Apply button and observe the effect of the new span factor. Repeat this step until a satisfactory reading is displayed.

4. The channel is now calibrated.

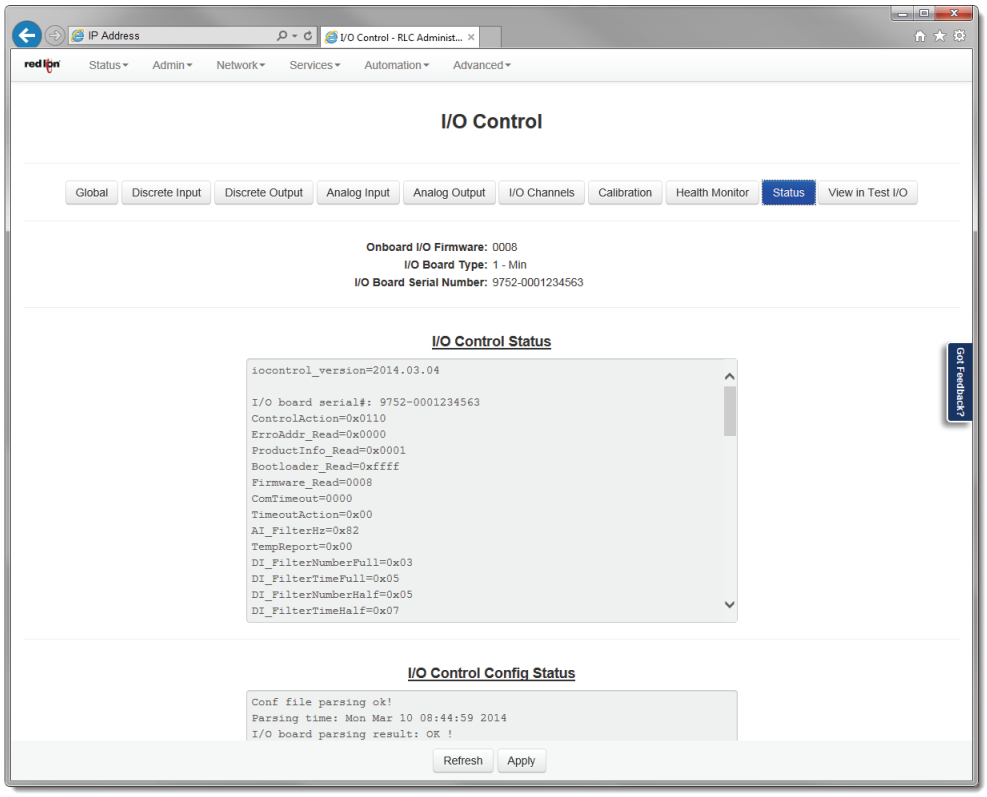
Health Monitor

- Click on the Health Monitor button and the dialog window below will appear. This dialog window will supply the user with feedback on the unit's temperature and power readings.



Status

- Click on the Status button and the dialog window below will provide you with your system's I/O Control Status and I/O Control Config Status.



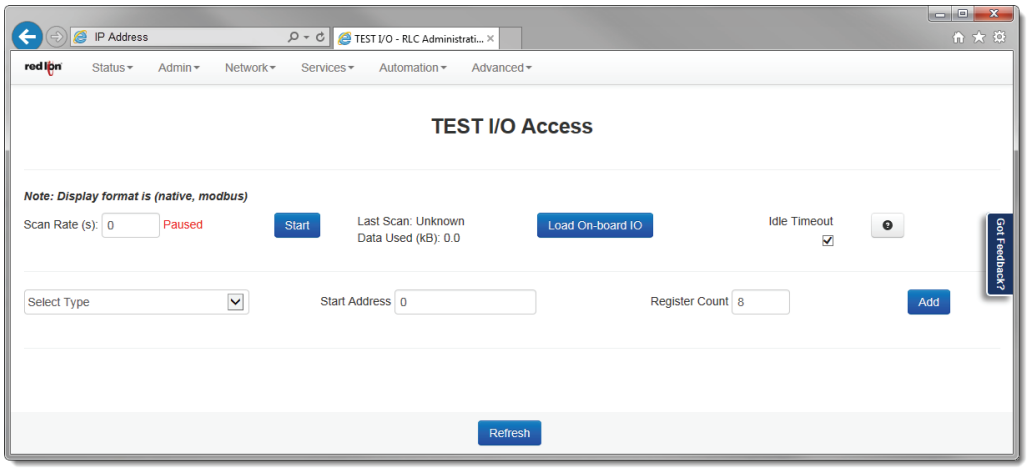
View in Test I/O:

- Click on the Test I/O button to be directed to the Test I/O Access dialog window. See section 3.6.5.2 for more information on this feature.

3.6.6.2 Test I/O

Test I/O is used to verify the functionality of I/O states in gateways, RTUs and I/O modules.

- Test I/O menu item and the following dialog window will appear:



The Test I/O interface has been kept simple to make managing the test I/O process easier and keep the screen less cluttered and easier to look at and quickly locate your test values.

Scan Rate: This is the time in which the screen will automatically refresh values from the internal I/ODB.

Idle Timeout: When this option is enabled, the browser will stop scanning after two minutes of inactivity.

Select Type: From the drop down list, select the type of I/O you would like to test. Valid I/O types are:

Analog In	Discrete In	Long In	Float In
Analog Out	Discrete Out	Long Out	Float Out

Start Address: Once the I/O type has been selected, enter the Start Address.

Register Count: Enter the Register Count.

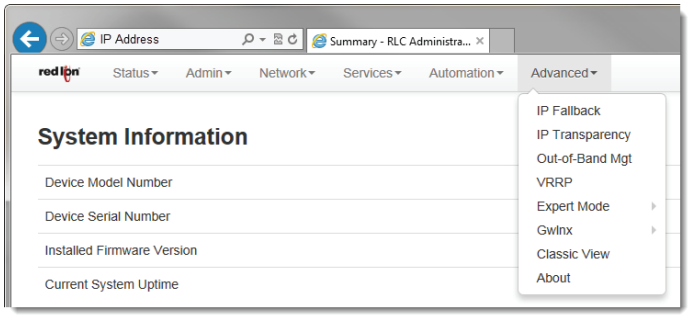
- Click on the Add button to test the I/O.

The messages log shows the range entered and each register that can be edited and monitored for the analog Inputs.

You may enter values here and observe your IODB data from another device / location to see those values get updated, or you may initiate a change from another device/input and observe the changes presented here on your Test I/O interface.

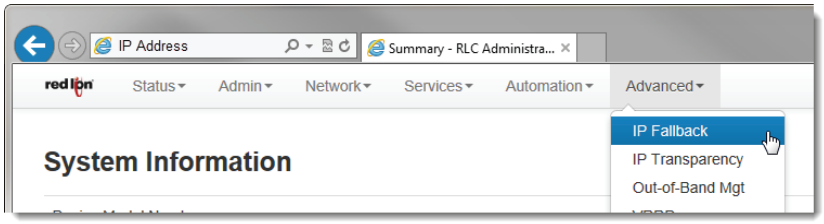
3.7 Advanced Tab

The Advanced Tab is used to configure the Red Lion router, which included IP Fallback, IP Transparency, Out-of-Band Management, VRRP, Sub-Systems and Gwlnx.



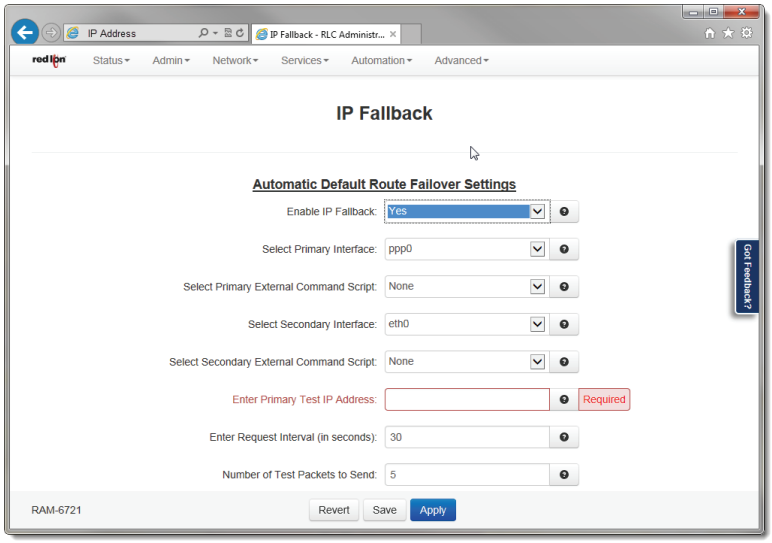
3.7.1 IP Fallback

IP Fallback is supported in Red Lion routers in the IndustrialPro and EnterprisePro series.



The IP Fallback option is used to configure the Red Lion router to failover between two interfaces, ex. Primary route on DLS/Cable on eth0, and secondary on Cellular if the primary loses Internet connection.

- Click on the IP Fallback menu item and the following dialog window will appear:



Enable IP Fallback: Select *YES* to enable the IP Fallback. Enable this option if you have two paths (interfaces) configured with WAN (internet) support. An example would be primary ethernet (eth0) and secondary wireless (ppp0). ***Note:*** *When using an ethernet port setup as DHCP Client, choose:* ***Use Remote Gateway as Default Route: NO*** *in the ethernet port setup screen. Default route control will be managed by the IP Fallback instead.*

Select Primary Interface: Specify your desired primary interface for IP Fallback behavior.

Select Primary External Command Script: Choose the name of the command script to be executed when the associated interface becomes active. For example, if a *RestartVPN* is an option, then when selected, it will be run whenever the fallback logic selects and activates this interface.

The recommended setting for this field is *None* for standard operation with no special behaviors. *RestartVPN* is useful when using and IPSEC VPN tunnel.

Select Secondary Interface: Select the secondary interface to be used for IP Fallback. Selecting vrrp will coordinate with the VRRP process, so that when the primary interface is determined to be unavailable, VRRP will stop broadcasting availability.

Select Secondary External Command Script: Choose the name of the command script to be executed when the associated interface becomes active. For example, if a *RestartVPN* is an option, then when selected, it will run whenever the fallback logic selects and activates this interface.

The recommended setting for this field is *None* for standard operation with no special behaviors. *RestartVPN* is useful when using an IPSEC VPN tunnel.

Enter Primary Test IP Address (Required): Specify the IP address of a host with which the IP Fallback service will communicate to test connectivity. Value must be a pingable address, and not a domain name. The best choice would be an address that represents end-to-end connectivity.

Enter Request Interval (in seconds): Specify the time, in seconds, to wait between connectivity tests. The minimum is 10, maximum is 600. **Note:** This value should be 30 or higher for PPP connections.

Number of Test Packets to Send: Specify the number of 0 byte ping packets to send out to test connectivity. The minimum is 2, maximum is 30. The recommended setting for this field is 5 - 10.

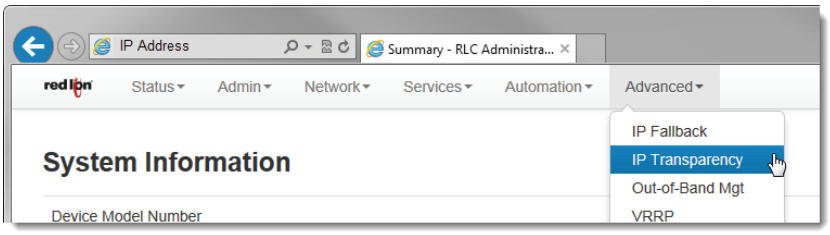
Allowable Test Packet Loss: Specify the number of lost packets that are acceptable before the IP Fallback service will consider the link unavailable, and switch to its secondary. Note: the value must be less than the number of test packets set via Test Packets to Send.

Select Debugging Level: Specify a debug level for logging purpose. This is recommended only when existing configurations do not function as expected, and when directed to change by Red Lion Technical Support.

- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

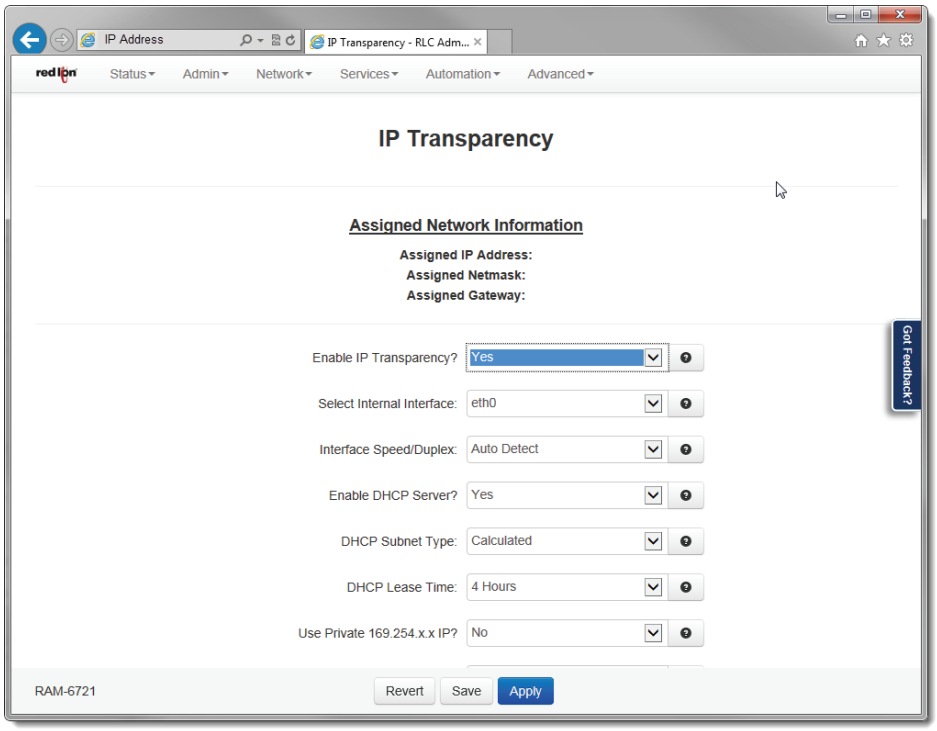
3.7.2 IP Transparency

IP Transparency is supported on Red Lion routers in the IndustrialPro and EnterprisePro series. The IP Transparency menu item is used to configure the transparent bridging capability of the Red Lion router.



IP Transparency is a special use capability. IP Transparency will take all inbound traffic to the Red Lion router and pass it transparently through to the interface specified. This is useful when it is desired to pass traffic to a legacy firewall, or VPN concentrator located behind the Red Lion router and not to use the firewall or VPN capabilities of the Red Lion router itself.

- Click on the IP Transparency menu item and the following dialog window will appear:



Enable IP Transparency: Select Yes to enable the IP Transparency feature. Settings will take effect immediately when the Apply button is clicked or after a reboot when Save is clicked. Note: Enabling IP Transparency will negate all configured firewall rules. The firewall and DMZ Host services will be disabled prior to using IP Transparency.

Select Internal Interface: Select the interface to be designated the “internal” interface by making the appropriate choice from the provided list. The wireless IP will be issued out of this interface.

Interface Speed/Duplex: Select the Speed and Duplex to be used for the physical interface. The recommended setting for this field is *Auto-Detect*. The following options are available:

- **Auto Detect:** Use the 'best negotiated' speed and duplex (default)
- **10 Mbps/Half:** Force the interface to 10 Mbps and half-duplex
- **100 Mbps/Half:** Force the interface to 100 Mbps and half-duplex
- **100 Mbps/Full:** Force the interface to 100 Mbps and full-duplex

Note: An incorrect 'forced' setting will result in communication failure for this interface.

Enable DHCP Server: Select Yes to allow the DHCP Server(s) to be enabled while IP Transparency is in effect.

DHCP Subnet Type: A calculated subnet will be based on the actual IP Address received from the wireless network. This option is more compatible with a wide variety of routers, but will mask out nearby IP addresses. This may make other IP's within the host network unreachable. Point-to-Point will use a /32 subnet, but is not compatible with some routers. The recommended setting for this field is *Calculated*.

DHCP Lease Time: Choose the time for DHCP Leases when issuing the Transparent IP. The recommended setting for this field is 4 hours.

Use Private 169.254.x.x IP: Select whether the internal IP Transparency interface will host a "dummy" gateway IP simulator to the IP Transparency IP, or if it will use a calculated 169.254.x.x IP Address. Some Cisco routers might not ARP properly when this option is turned on.

> **Pros:** Option turned Off may allow some Cisco routers to ARP better.
>
> **Cons:** With the option turned Off, the unit will black hole some IPs, and they will not be reachable from the device behind. Example: IP from ISP is 1.2.3.3. Calculated Mask is 1.2.3.2/30. Now IPs 1.2.3.0, 1.2.3.1 and 1.2.3.2 become unroutable beyond the device.

Allow TELNET access to this device: Select Yes to allow TELNET access to this device. Incoming connections on the specified port will be directed internally to port 23, instead of to the device behind the specified Internal Interface. *Note: For this option to function properly, the TELNET Server must be enabled on port 23 via the Services tab.*

Allow SSH access to this device: Select Yes to allow SSH access to this device. Incoming connections on the specified port will be directed internally to port 22, instead of to the device behind the specified Internal Interface. *Note: For this option to function properly, the SSH Server must be enabled on port 22 via the Services tab.*

Allow SNMP access to this device: Select Yes to allow SNMP access to this device. Incoming connections on UDP port 161 will be directed internally to port 161 instead of to the device behind the specified Internal Interface. *Note: For this option to function properly, the SNMP Agent must be enabled via the Services tab.*

Allow access to Web UI: Select Yes to allow access (for incoming TCP Port 10000 connections) to the Web UI on this device. Selecting No will allow the connection through to the device behind the selected interface. The recommended setting for this field is *Yes*.

Enter Web UI Port (Required): Enter the TCP Port number to be used for Web UI access when Web UI access has been enabled. The port chosen will be redirected locally (to internal 10000). Connections on this port number will not reach the device behind the specified Internal Interface. The recommended setting for this field is 10000. All Web UI traffic will be redirected locally to port 10000 automatically. This behavior is built-in and not configurable.

Allow access by SixView Manager: Select *Yes* to allow access (for incoming TCP Port 7785 connections) to trigger this device for remote check-in by the SixView Manager server. Selecting No will allow the connection through to the device behind the selected interface. The recommended setting for this field is *Yes*.

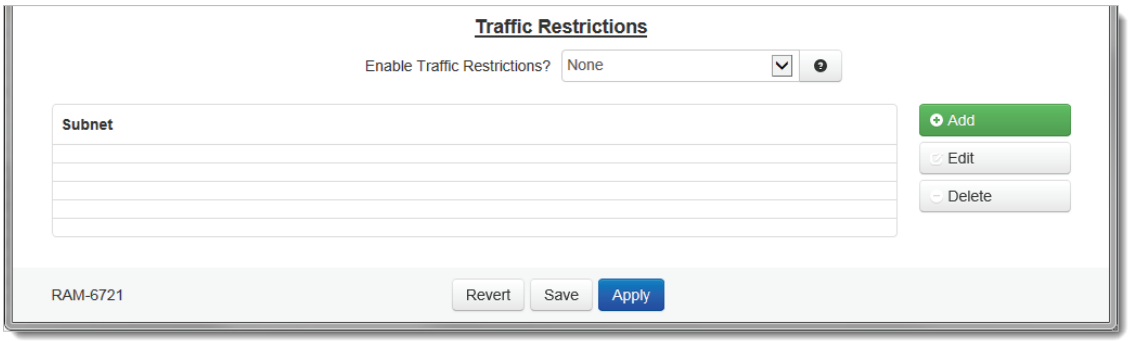
Enter MAC filter: Enter a valid MAC address using the following format: *nn:nn:nn:nn:nn:nn*, where *nn* is a number in hexadecimal form (0-9, a-f, A-F) to enable a MAC filter for use with IP Transparency. A MAC filter allows only packets whose MAC address matches the filter value to be passed thru this device. Leaving this field empty effectively disables MAC filtering.

Enable Out-of-Band Port Redirect: Select *Yes* to allow any Out-of-Band ports to be redirected locally to this device. When enabled, the OOB Ports specified in the Advanced->Out-of-Band Mgt section will be automatically allowed. The recommended setting for this field is *Yes*, when also configuring Out-of-Band Mgt on this unit.

Enable Port Redirecting: Select *Yes* to allow redirecting of ports to a device beyond this device (the one being configured). Example: A device beyond the IPT device is running a WEB server on port 80, but an upstream router is blocking Port 80. Redirecting traffic to another port, say 8080, will allow communication with the server. This would be setup as our External port 8080 redirected to an Internal Port 80, Protocol TCP.

When this feature is enabled, a new field will appear containing a table into which multiple entries can be entered. Each entry will include the External and Internal Port numbers and a traffic type (TCP or UDP).

Enable Traffic Restrictions: Select *Yes* to restrict traffic to a device beyond this device (the one being configured). When this feature is enabled, a Traffic Restrictions table will appear to allow selection of the restriction mode and a table into which multiple entries can be entered. Each entry will specify the network IP address range to which the restrictions will be applied.



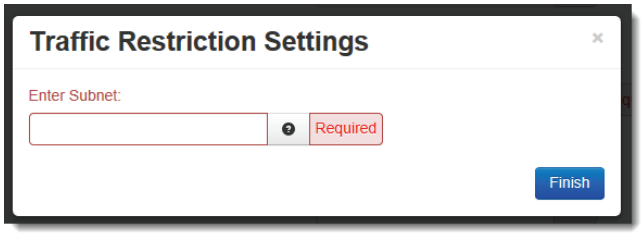
Enable Traffic Restrictions: This field is enabled when "Enable Traffic Restrictions" has been set to Yes. Select the restriction mode from the list provided.

None: No filtering is performed.

Only: Allow connections to/from the associated subnet list only. (inbound and Outbound Restrictions)

In: Allow new incoming connections from the associated subnet list only, but allow any originating outbound connections from the host behind the Red Lion router. (Inbound Restriction)

- Click on the Add button and the following window will appear:



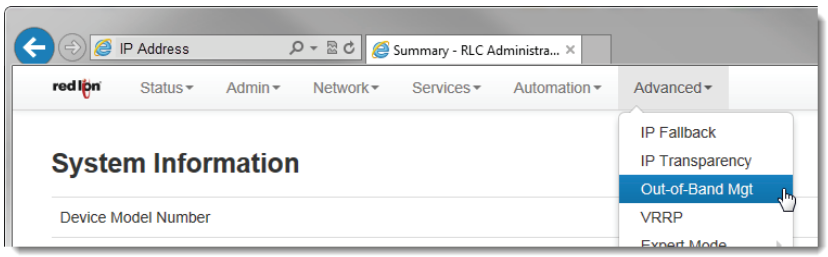
Enter Subnet (Required): Enter subnet range for which to restrict traffic in the CIDR form *nnn.nnn.nnn.nnn/xx*, where *nnn* is the IP Address and *xx* is the subnet in Network Bits format.

- Click on the Finish button to populate the Table Restrictions screen.

- To delete an existing item, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the “Save” button for changes to be saved without activating the interface until you reboot the unit, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

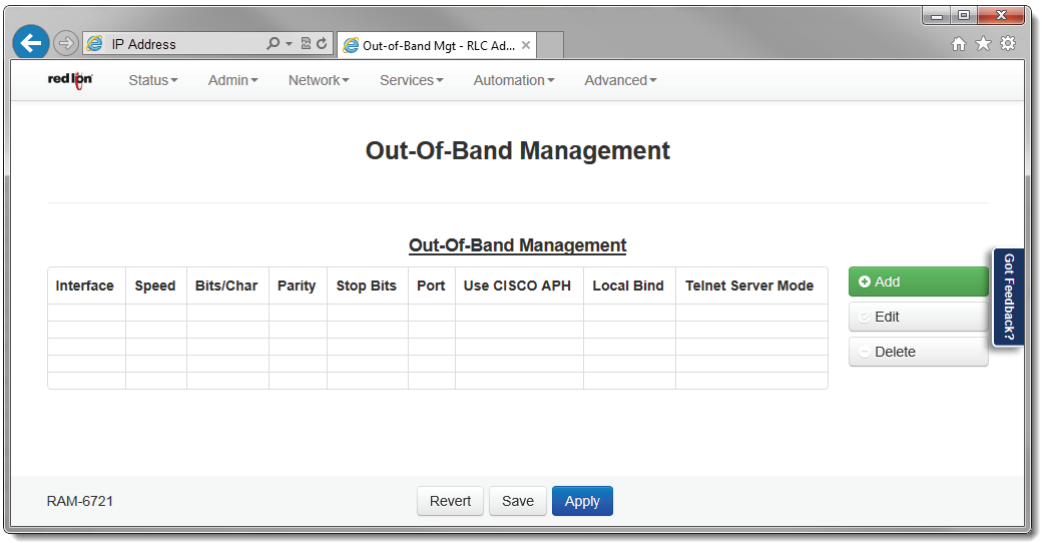
3.7.3 Out-of-Band Management

The Out-of-Band Management menu item is used to configure the capability of remotely administrating a third-party device connected via a serial cable on the Red Lion router.

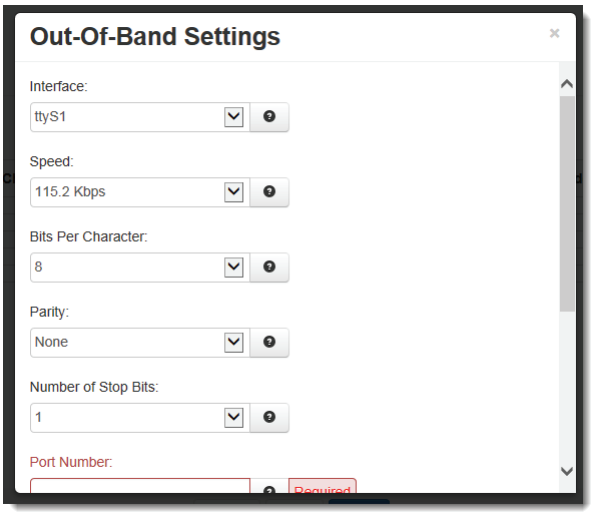


Note: *Please refer to the third-party device user manual and/or technical support to determine what type of connection is required to connect with the Red Lion router from the RS232 serial port.*

- Click on the Out-of-Band Mgt menu item and the following dialog window will appear:



- Click on the Add button to add an instance for OOB Management and the following window will appear:



Interface: Select the interface to used.

Note: For Speed, Bits, Parity and Stop Bits, consult the configuration of the remote device being attached; this setting must be compatible.

Speed: Select the desired interface speed to be used.

Bits per Character: Select the word length (bits per character) to be used.

Parity: Select the parity to be used. Consult the configuration of the remote device being attached, this setting must be compatible.

Number of Stop Bits: Select the number of stop bits to be used. Consult the configuration of the remote device being attached, this setting must be compatible.

Port Number (Required): Enter a valid port number (1-65535) to be used for the connection.

Take care to choose a port number not already used by other system services. Consult the **Status>Network>Socket Statuses> TCP Only** menu for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access in Network>Firewall>Port Allow/Forwarding Rules>Service Access Rules.

Use CISCO APH: Select *Yes* to enable the CISCO APH or *No* to prevent it's use. The recommended setting for this field is Yes when connecting to a Cisco console port.

Use Local Binding: Select *Yes* to enable Local Binding. Local Binding will prevent remote access to this port. You will be required to Telnet/SSH to the unit's command line, and then Telnet to the OOB port locally (telnet localhost<OOB Port>).

Telnet Server Mode: This option controls how some options negotiations will be performed with a TELNET client. Recommended setting is "Basic + drop LF & NUL" is a commonly utilized setting. The following options are available:

Disabled: No TELNET options negotiation is performed.

Basic: Common TELNET options negotiation is performed.

Basic + drop LF: Line feed characters (x'0A) are dropped.

Basic + drop LF & NUL (Cisco Preferred): LF and NUL (x'00) characters are dropped.

Basic + drop LF & NUL/HIGH: LF, NUL and any characters > x'7F are dropped.

Basic + drop CR: Carriage return characters (x'0D) are dropped.

Basic + drop CR & NUL: CR and NUL (x'00) characters are dropped.

Basic + drop CR & NUL/HIGH: CR, NUL (x'00) and any characters > x'7F are dropped.

Note: *Selecting the right value for your particular situation may require some experimentation.*

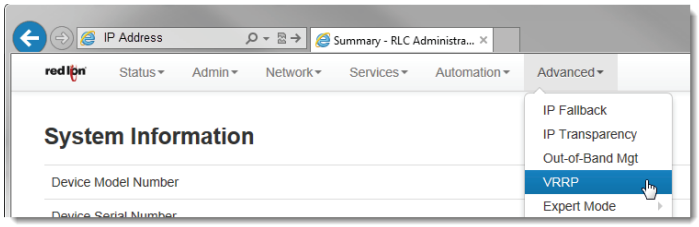
The Basic Telnet Server will enable some telnet negotiation options with common Telnet Clients, which may provide a better user experience. If you are having problems with odd echoed characters, or other interactive problems, please enable this option.

If you are having problems with login not accepting your password, or pressing "Enter" seems to behave as if two Enter keys have been pressed, try one of the "Drop" options.

- Click on the Finish button to populate the Out-of-Band Management screen.
- To delete an existing item, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.
- Click on the "Save" button for changes to be saved without activating the interface until you reboot the unit, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

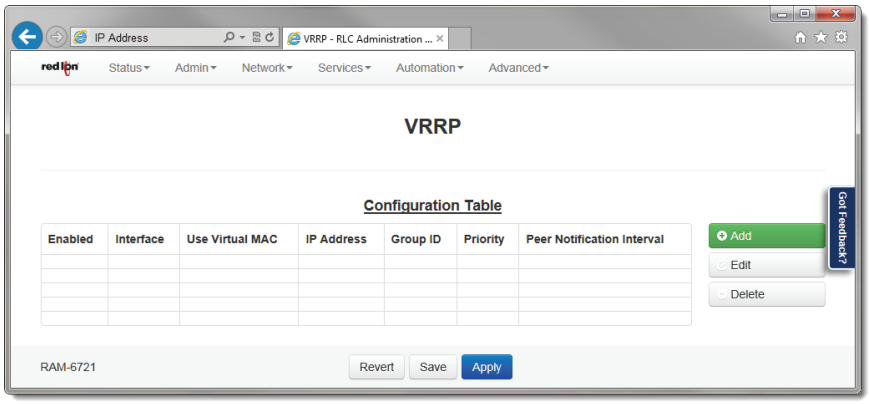
3.7.4 VRRP (Virtual Redundancy Protocol)

VRRP is supported in Red Lion routers in the IndustrialPro and EnterprisePro series. To configure VRRp, select the option from the Advanced menu.

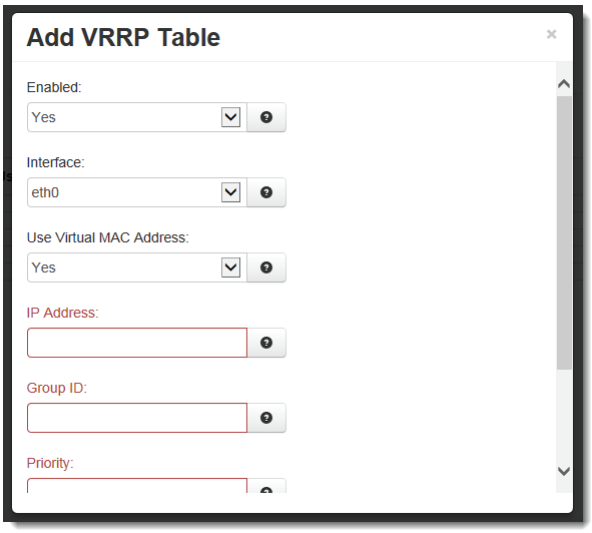


The VRRP menu item allows you to configure the capability of providing redundancy capabilities to each other as well as other third party devices.

- Click on the VRRP menu item and the following dialog window will appear:



- Click on the Add button and the following dialog window will appear:



Enabled: Specify whether you want to enable the VRRP service on this device. The service will be started after clicking the Apply, and on each subsequent boot. VRRP is designed to work with multiple systems. Enable only if you intend to setup other VRRP partners.

Interface: Specify the interface the VRRP service should use for communication.

Use Virtual MAC Address: Specify whether you want to allow the VRRP service to handle virtual MAC addresses. The recommended setting for this field is YES.

IP Address: Specify the IP address of the virtual server. This value must not be currently assigned to any other network interface on the subnet. Furthermore, this value must match in any VRRP partner's configuration for redundancy to operate correctly.

Group ID: Specify the ID number of the virtual server. This value must match in any VRRP partner's configuration for redundancy to operate correctly. Multiple VRRP Virtual interfaces can operate on the same subnet, as long as each set of redundant partners uses a different ID.

Priority: Specify the priority to use in VRRP negotiations. Valid values are 1-255. Note: If this is the "Master" device, the priority should be sent higher than the "Backup" device.

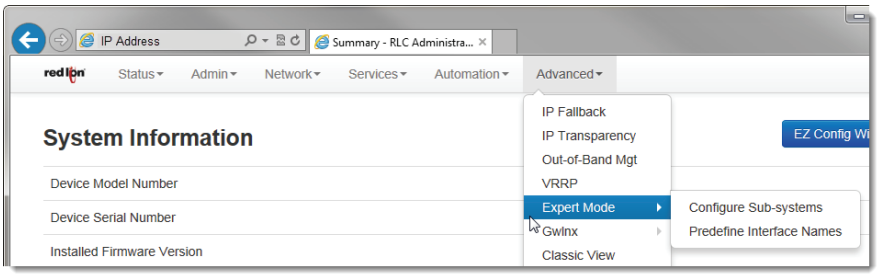
Peer Notification Interval: Specify the amount of time, in seconds, between VRRP broadcast packets.

- Once you have entered the desired default settings for the VRRP, click on the Finish button and you will return to the VRRP dialog window. The Configuration Table will be populated with the information entered.
- To modify settings, select the line to be edited and click the Edit button. To remove settings from the table, select the desired line and click on the Delete button.
- Click SAVE to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

3.7.5 Expert Mode

The Expert Mode menu allows you to edit the configuration fields of Red Lion IndustrialPro/EnterprisePro router directly. This option provides the ability to perform advanced configuration capabilities for complex organizations.

Note: Expert Mode is not recommended unless directed by Red Lion Technical Support.

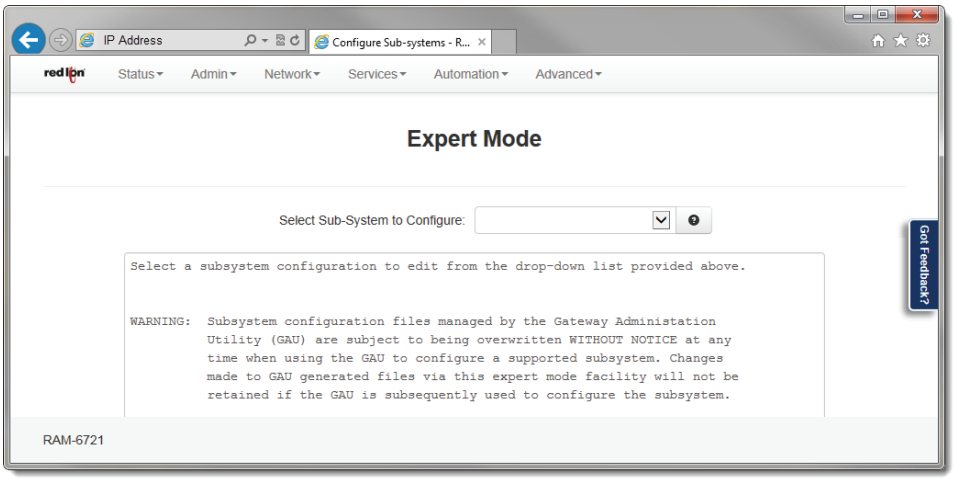


WARNING: Should you choose to edit the configuration files directly, we encourage you to contact Red Lion Technical Support. Once you have manually edited a configuration file without the use of the Web UI, you should refrain from any further configurations to that subsystem through the Web UI, as it will overwrite any changes you may have made.

3.7.5.1 Configure Sub-Systems

The “Configure Sub-Systems” menu item allows you to edit the main configuration files of the Red Lion router. It is not recommended that you perform configuration activities using this facility unless instructed to do so by Red Lion Technical Support.

- Click on the Configure Sub-System menu item and the following window will appear:


IP Address
Configure Sub-systems - R...
Status
Admin
Network
Services
Automation
Advanced
Expert Mode
Select Sub-System to Configure:
Select a subsystem configuration to edit from the drop-down list provided above.
WARNING: Subsystem configuration files managed by the Gateway Administation Utility (GAU) are subject to being overwritten WITHOUT NOTICE at any time when using the GAU to configure a supported subsystem. Changes made to GAU generated files via this expert mode facility will not be retained if the GAU is subsequently used to configure the subsystem.
RAM-6721
Got Feedback?

Select Sub-System To Configure: Select a component sub-system from the list as directed by Technical Support. Your choice will load the given sub-system’s configuration file into the text box for editing. The following controls (buttons) are available:

Cancel: Reload the file in the text box, removing all unsaved changes.

Default: Load a default file in to the text box for editing. All changes to the defaults file will be reflected in the “real” (rather than the default) configuration file.

Save: Save the contents of the text box in to the “real” sub-system configuration file.

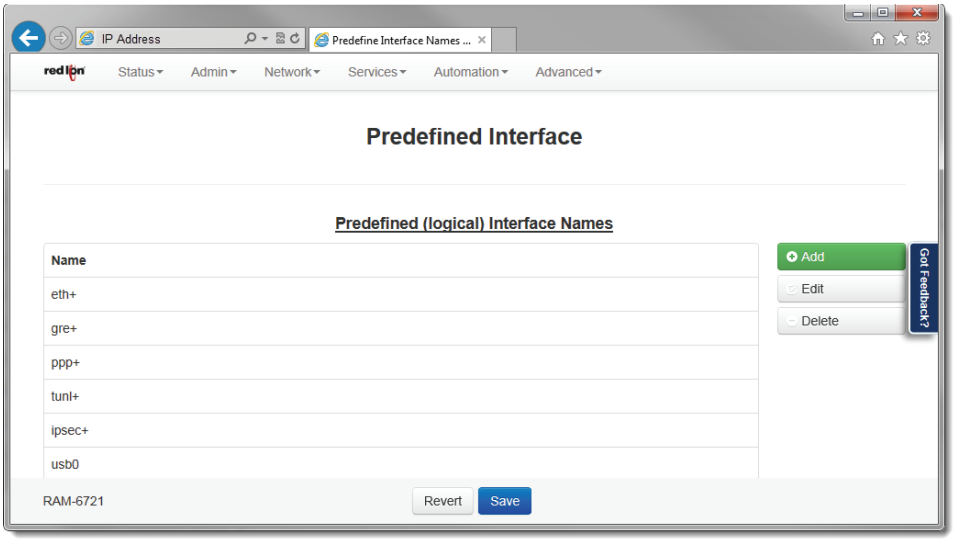
Stop: Stop the component sub-system service if it is currently running.

Start: Start the component sub-system service, or re-start it if it is currently running. Some may need a Stop first.

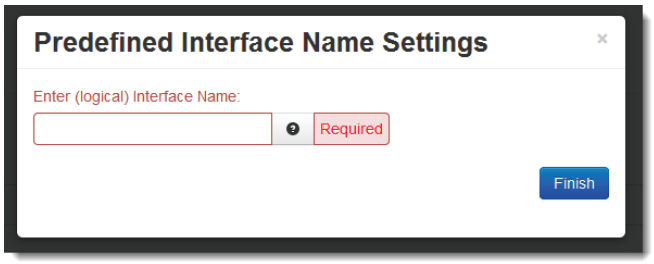
3.7.5.2 Predefined Interface

The Predefined Interface Names menu item allows you to create a named interface for use in applications such as OpenVPN that require a logical interface, i.e. tun0 that the Red Lion does not know about. Using the Predefined Interface Name will place the name of the interface into the pull-down menus of interface selections to be used by the system.

- Click on the Predefined Interface Names menu item and the following dialog window will appear:



- Click on the Add button to add a named interface and the following pop-up window will appear:

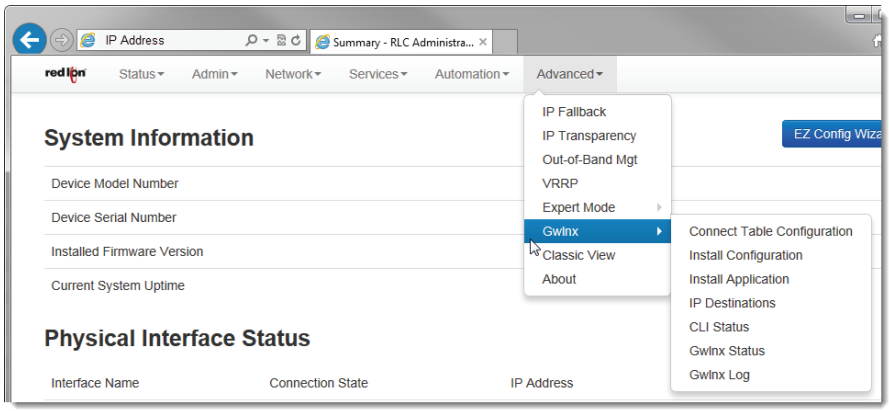


Enter (logical) Interface Name (Required): Enter the name of the interface to be used for the logical interface. For example: tun0, gre4, ppp100, etc.

- Click on the Finish button to populate the Predefined Interface Names screen.
- Click SAVE to store the settings for the next reboot. Selecting Revert, will reset all fields to the previously saved defaults.

3.7.6 Gwlnx

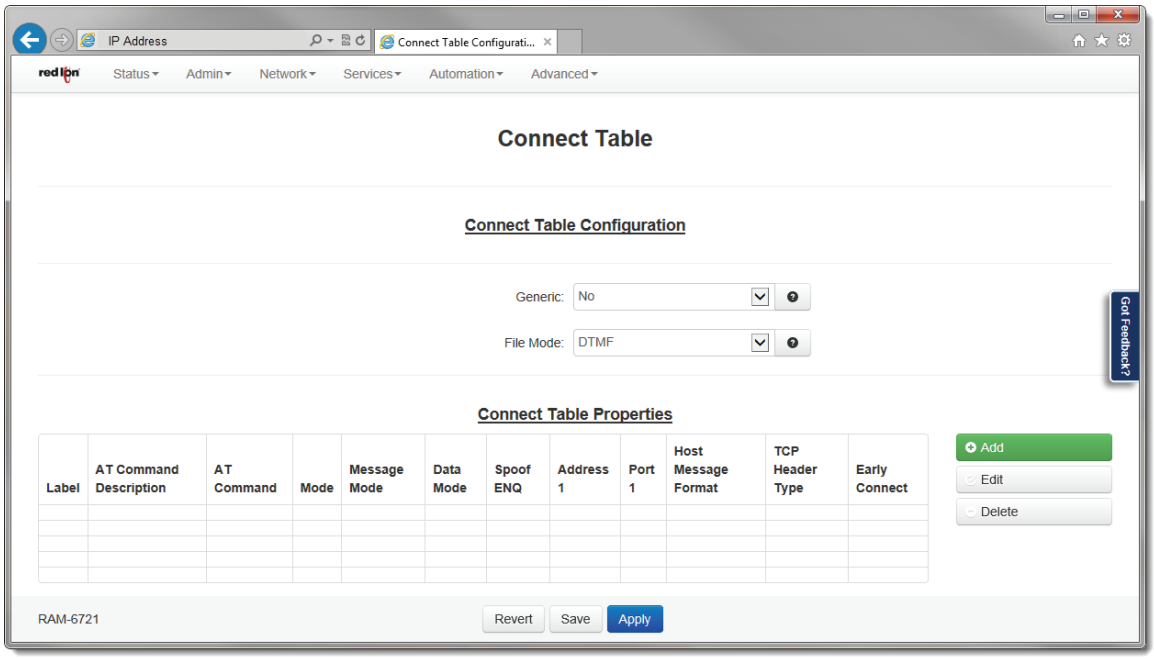
The Gwlnx menu item is used to define the following sub-menus: Connect Table Configuration, Install Configuration, Install Application, IP Destinations, CLI Status, Gwlnx Status and Gwlnx Log.



3.7.6.1 Connect Table Configuration

The Connect Table Configuration menu item is used to configure the communication ports behavior via Serial or Modem using Dialed Number Identification Service (DNIS) method.

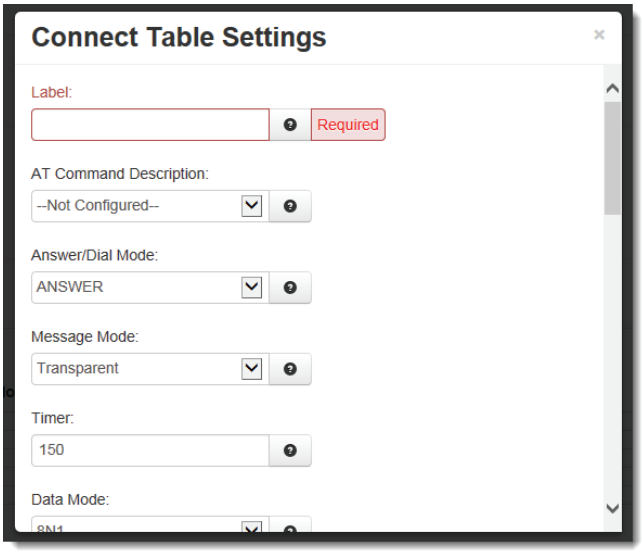
- Click on the Connect Table Configuration menu item and the following dialog window will appear:



Generic: Please use the recommended setting unless directed to change by Red Lion Technical Support. The recommended setting for this field is No.

File Mode: Please use the recommended setting unless directed to change by Red Lion Technical Support. The recommended setting for this field is DTMF.

Connect Table Properties: To create a table setting, click on the Add button and the following dialog window will appear:



Label (Required): Enter the Lookup Key associated with this entry. This is commonly a phone number, or a portion of a phone number for partial matches of incoming calls. (i.e. “18” will match 1-800-xxx-xxx, 1-888, 1-866 and similar numbers.) The recommended setting for this field is 1001.

A value of “default” will designate this entry as the option to use if no other entry matches. If no “default” label exists, the first entry in the list will be the default and match any incoming number received.

For a Dial/Ring-Out Mode, this field should match the phone number entered in the Com Port Manager configuration for Gwlnx TCP Server port number, if using a dynamic TCP Listening Port.

AT Command Description: The best choice is often determined by previous testing with a particular model/brand of connecting device. The first three “Direct” options are the most commonly used. The recommended setting for this field is Direct 1200 Bell212 = At&Q6+MS=B212

If choosing a User Defined option, enter the full AT command. Below is a list of AT Commands:

- Direct 1200 Bell212 = AT&Q6+MS=B212
- Direct 1200 V22 = AT&Q6+MS=V22
- Direct 2400 V22bis = AT&Q6+MS=V22B
- Direct2 1200 Bell212 = AT\NO+MS=B212
- Direct2 1200 V22 = AT\NO+MS=V22
- Direct2 2400 V22bis = AT\NO+MS=V22B
- ErrorC 1200 Bell212 = AT\N3+MS=B212
- ErrorC 1200 V22 = AT\N3+MS=V22
- ErrorC 2400 V22bis = AT\N3+MS=V22B

Answer/Dial Mode: For incoming calls, choose “ANSWER_2WAY_RAW”. For outbound (Ring Out/Ring Down) mode, choose “DIAL”. The other options should only be used if instructed to do so by Red Lion Technical Support. The recommended setting for this field is ANSWER_2WAY_RAW.

Message Mode: This will choose between enabling the local VIsa protocol engine or allowing Passthru/Transparent mode. The recommended setting for this field is Transparent.

Transparent: Allow raw communication between the Dial port and the TCP Connection.

Visa: Enable local Visa I engine. This will process one transaction, and issue an EOT after the transaction response has been sent to the dial device.

Visa2: Enable local Visa II engine. After a transaction is complete and ENQ will be issued to query the next transaction in sequence. If there is no response to the ENQ, then an EOT is issued.

Timer: Transparent Mode is the inter-character delay (in milliseconds) used on the serial side to determine when a remote device is finished transmitting. A low value may generate a faster response, but can send many TCP packets and 'fragment' the serial data packets. A higher value will collect a larger amount of data into a single TCP packet, and will generally keep packet boundaries more intact. Visa mode is unused. The recommended setting for this field is 150 for Transactions and 10 for some Streaming Protocols (ATM Management Protocols).

Data Mode: The following data mode is supported:

8N1: Data will be treated as full 8 bits valid. If the serial device is transmitting 7E1, then 7E1 formatted data will be transmitted to the TCP side.

7E1: Process data as if in 7E1 format. If the serial device is transmitting 7E1, then appropriate parity will be stripped/added so that communication on the TCP side will be in 8N1.

The recommended setting for Transparent mode: As needed for various serial devices and TCP hosts.

The recommended setting for Visa mode: Leave this setting at 8N1. Automatic 7E1 detection is used.

Spoof ENQ: The recommended setting for this field is *No*.

Transparent Mode: This will enable an ENQ packet to be sent to the serial device to initiate a transaction. Up to 5 ENQ's will be sent while waiting.

Visa Mode: Unused. The Visa engine will automatically issue ENQ's as needed, according to the Gwlnx config file.

No Rx Before Tx: Discarding data before transmitting in supported Message Mode. The recommended setting for this field is *No*.

Transparent Mode: This will discard any data received from the serial side, prior to transmitting some data to the remote serial device. This can be useful to discard initial line noise remnants from modem connections before an ENQ is issued (or other start-data message types from a TCP host).

Visa Mode: Unused. This is automatically enabled in the Visa engine, as it awaits a STX.

Disable Ack: Acknowledgement behavior in supported Message Mode. The recommended setting for this field is No.

Transparent Mode: Unused.

Visa Mode: Once a message is received from the serial device (ATM/POS) and the LRC is valid, this will disable sending an ACK. Certain ATP/POS devices will fail if sent an ACK, and rather use the response message from the TCP host as an implied ACK. Certain ATM/POS devices require an ACK before receiving the response message from the TCP host.

Pass Through Ack: Passing Acknowledgement in supported Message Mode. The recommended setting for this field is No, unless using a SmartConnect device at the host processing side.

Transparent Mode: Unused.

Visa Mode: When an ACK is received from an ATM/POS device, pass that up to the host processor.

Enter IP Address 1 (Required): For coordination with SSL Connections, use 127.0.0.1. When using ANSWER mode, this is a Client Primary IP address that GWLNX uses to connect to the Host server. When using DIAL mode, this field is not used.

Enter Port 1 (Required): This is a Client Primary Port address that GWLNX uses to connect to the Host Server Port. For coordination with SSL Connections, this field should match the "TCP Listening Port" configured in Services->SSL Connections->SSL Client, to reach the specified remote SSL Host Server.

When using DIAL mode, and Gwlnx is configured for Dynamic TCP Server Listener Port, this field will specify the TCP Port to listen on.

The recommended setting for this field is 1000.

Enter IP Address 2: This is a Client First Alternative IP Address that Gwlnx uses to connect to the Host Server.

Enter Port 2: This is a Client First Alternative Port Address that Gwlnx uses to connect to the Host Server Port.

Enter IP Address 3: This is a Client Second Alternative IP Address that Gwlnx uses to connect to the Host Server.

Enter Port 3: This is a Client Second Alternative Port Address that Gwlnx uses to connect to the Host Server Port.

Host Message Format: Following are the host message formats in supported Message Mode. The recommended setting for this field is Default.

Transparent Mode: Unused.

Visa Mode: This describes the format expected by the TCP host processor of Visa transactions. Visa Messages from the AMT/POS device will conform to: STX - PAYLOAD - ETX - LRC

Default: Use the current settings in the Gwlnx configuration.

Payload Only: Strip Visa header/trailers. Send only the Payload.

Payload - ETX: Strip the Visa header and LRC block check.

STX - Payload - ETX - LRC: Strip only the LRC block check.

STX - Payload - ETX - LRC: Send the fully formatted Visa message.

Header Type: The TCP connection to a host may required length headers. This will optionally be prepended to the data received from the serial side, for either transparent or Visa Mode. The recommended setting for this field is *Default*.

Default: Use current Gwlnx configuration.

None: Use no headers.

JBM Standard: Use JBM Standard Headers. This will prepend a Two Byte Length (2BL) Header to the data, indicating the number of bytes in the message, not including the header bytes. Messages from the host must also have the 2BL header to be received properly.

Example: With the Host Message Format set to STX-Payload-ETX, and just JBMSTD Headers used, the TCP message sent to the Host will be: XX XX STX Payload ETX. Where XX XX would be the length of the payload data, plus 2 (STX and ETX bytes). If Payload was 296 bytes, then the 2BL would be 01 2A (in Hex).

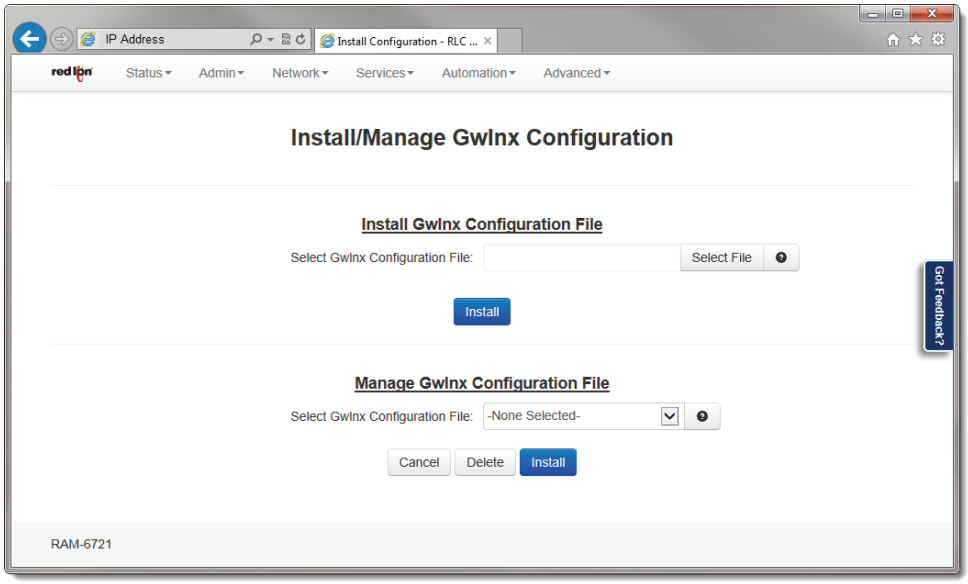
Allow Early Connect: Only adjust this option if directed by Red Lion Technical Support. The recommended setting for this field is *Yes*.

- Click on the Finish button and you will be directed to the Connect Table dialog window and the Connect Table Properties table will be populated with the entered data.
- Click on the "Save" button for changes to be saved without activating the interface, the "Apply" button will save your settings and apply them immediately. To revert to the previous defaults, click on the "Revert" button.

3.7.6.2 Install Configuration

The Install Configuration menu item is used to install the new Gwlnx configuration on Red Lion IndustrialPro or R-Series router devices. The Manage Configuration section is used to install or delete Gwlnx configuration files that already reside on Red Lion IndustrialPro or R-Series router devices.

- Click on the Install Configuration menu item and the following dialog window will appear:



Install Gwlnx Configuration File:

Select Gwlnx Configuration File: Click the 'Select File' button to select a Gwlnx configuration file to upload from your local system. It is recommended that you do not upload new files unless directed by Red Lion Technical Support.

Manage Gwlnx Configuration File:

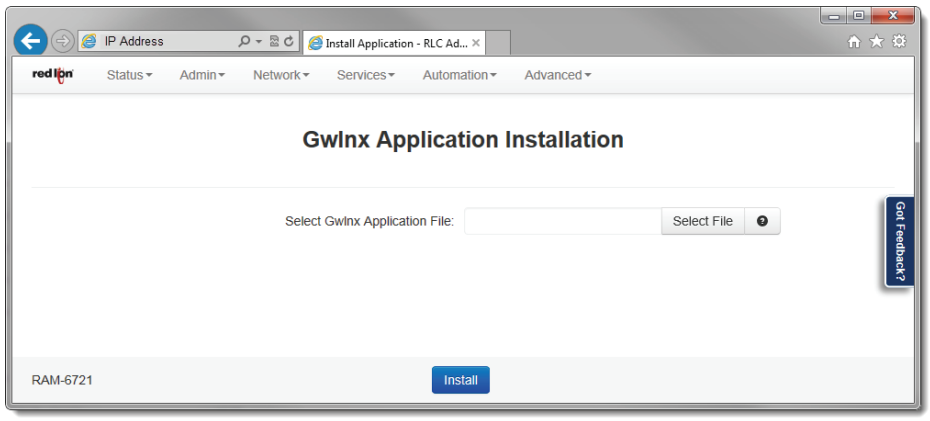
Select Gwlnx Configuration File: Select a Gwlnx configuration file on the remote unit to install or to delete. It is recommended that you do not install or delete files unless directed by Red Lion Technical Support.

Warning: *Deleting the 'unit.cfg' file may result in the 'gwlnx' application from not running on the next restart.*

3.7.6.3 Install Application

The Install Application menu item is used to configure the new Gwlnx application on Red Lion IndustrialPro or R-Series router devices.

- Click on the Install Application menu item and the following dialog window will appear:

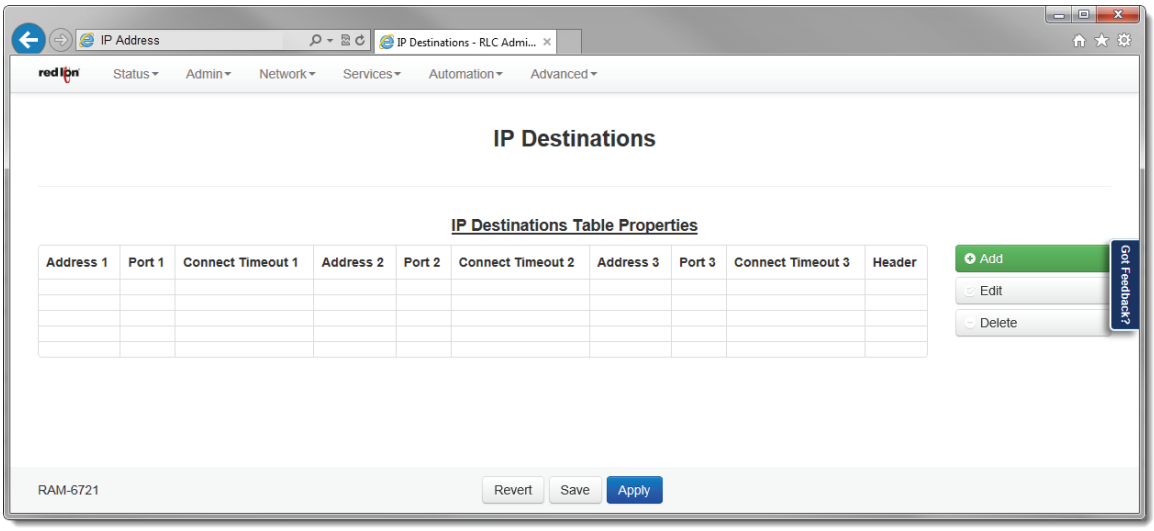


Select Gwlnx Application File: Click on the Select File button to select a 'Gwnlx' zip file to upload from your local system. It is recommended that you do not upload files unless directed to do so by Red Lion Technical Support.

3.7.6.4 IP Destinations

The IP Destinations menu item is used to configure the host processor (Server) IP/Port Addresses that Gwlnx application uses for TCP/IP communication protocol.

- Click on the IP Destinations menu item and the following dialog window will appear:



- Click on the Add button to define IP Destination Settings. The following dialog window will appear:

Enter Address 1 (Required): This is a Client Primary IP Address that Gwlnx uses to connect to the Host Server.

Enter Port 1 (Required): This is a Client Primary Port Address that Gwlnx uses to connect to the Host Server Port.

Connect Timeout 1 (Required): Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. Valid range is 2 -250 seconds. The recommended setting for this field is 10 seconds. A value less than 10 seconds is not recommended for a wireless environment

Enter Address 2: This is a Client First Alternative IP Address that Gwlnx uses to connect to the Host Server.

Enter Port 2: This is a Client First Alternative Port Address that Gwlnx uses to connect to the Host Server Port.

Connect Timeout 2: Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. Valid range is 2 - 250 seconds. The recommended setting for this field is 10 seconds. A value less than 10 seconds is not recommended for a wireless environment.

Enter Address 3: This is a Client Second Alternative IP Address that Gwlnx uses to connect to the Host Server.

Enter Port 3: This is a Client Second Alternative Port Address that Gwlnx uses to connect to the Host Server Port.

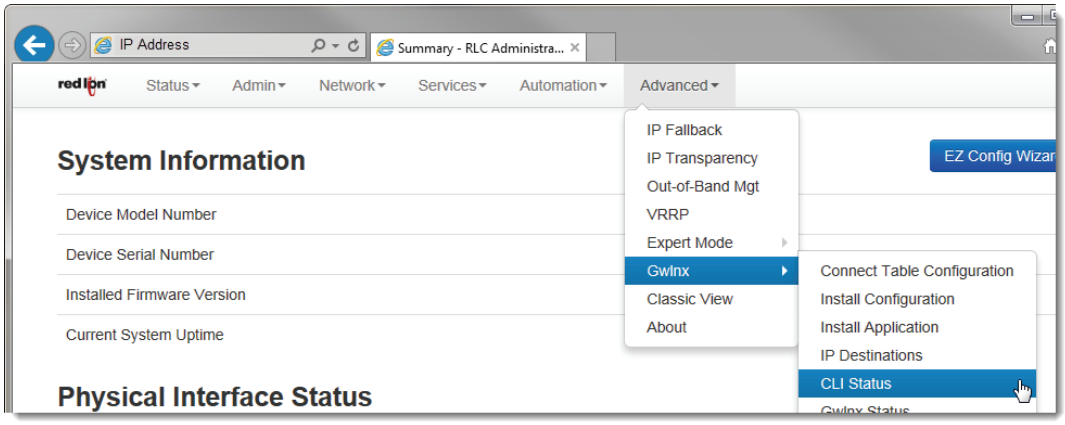
Connect Timeout 3: Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. Valid range is 2 - 250 seconds. The recommended setting for this field is 10 seconds. A value less than 10 seconds is not recommended for a wireless environment.

Header Type: This is a Header Length used in TCPIP packet that contains the Message Length being Send or Receive. The recommended setting for this field is Default.

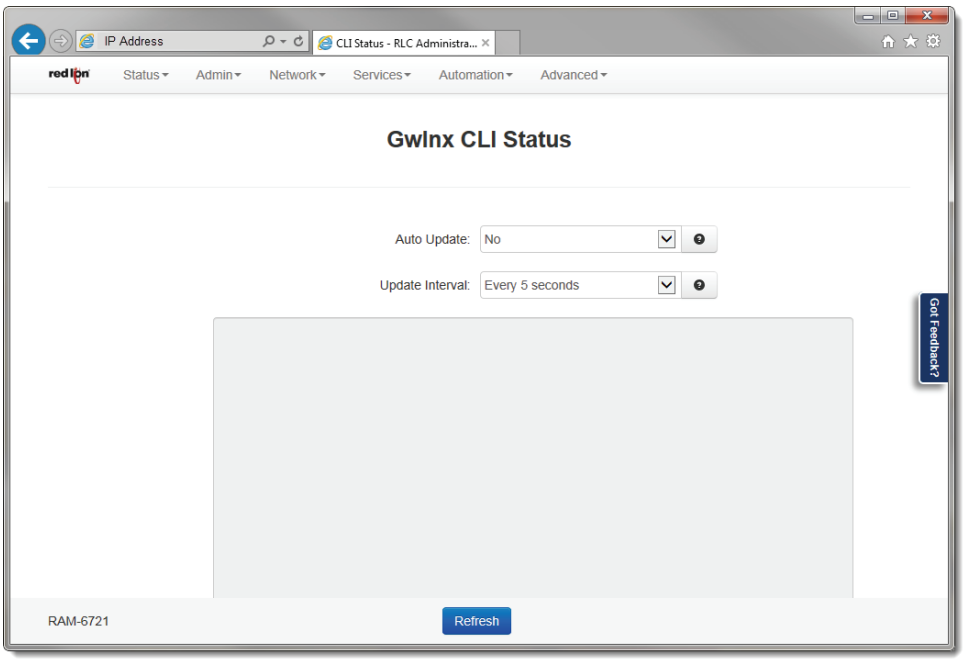
- Click on the Finish button and you will be directed to the IP Destinations dialog window and the IP Destinations Table Properties will be populated with the entered data.
- Click on the “Save” button for changes to be saved without activating the interface, the “Apply” button will save your settings and apply them immediately. To revert to the previous defaults, click on the “Revert” button.

3.7.6.5 CLI Status

The CLI Status menu item is used to view the status of the ports defined in the Gwlnx configuration file if the Gwlnx application is running.



- Click on the CLI Status menu item and the following dialog window will appear:



Auto Update: Select Yes to enable automatic updating of the log file display, the update interval can be selected using the Select Update Interval provided immediately below this control. Manual updating is disabled while auto-update is in effect. The current filter and maximum lines to be displayed will be used.

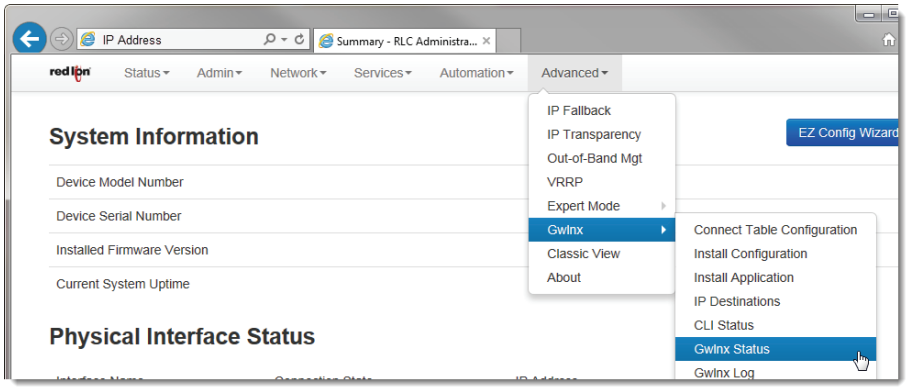
Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

Update Interval: Select the update interval to be used when auto-update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 5, 15, 30 & 60.

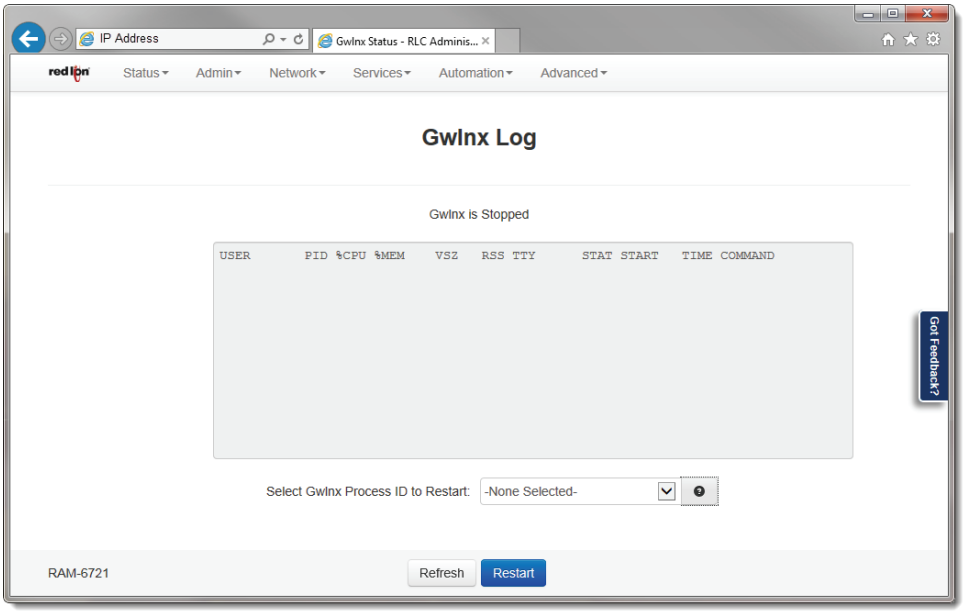
Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

3.7.6.6 Gwlnx Status

The Gwlnx Status menu item is used to view the Gwlnx process ID and has the ability to restart the application by selecting the process ID from the provided drop-down list. The Refresh button will refresh the process ID, if the Gwnlx application has been restarted.



- Click on the Gwlnx Status menu item and the following dialog window will appear:

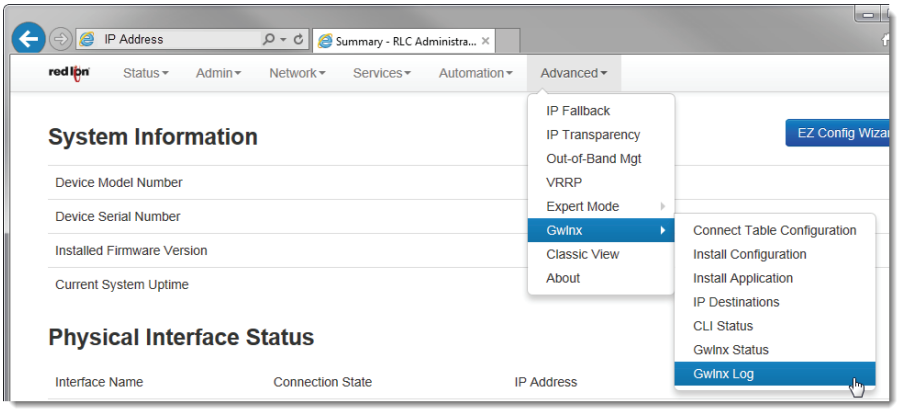


Select Gwlnx Process ID to Restart: Select the Gwlnx Process ID (PID) that you would like to restart.

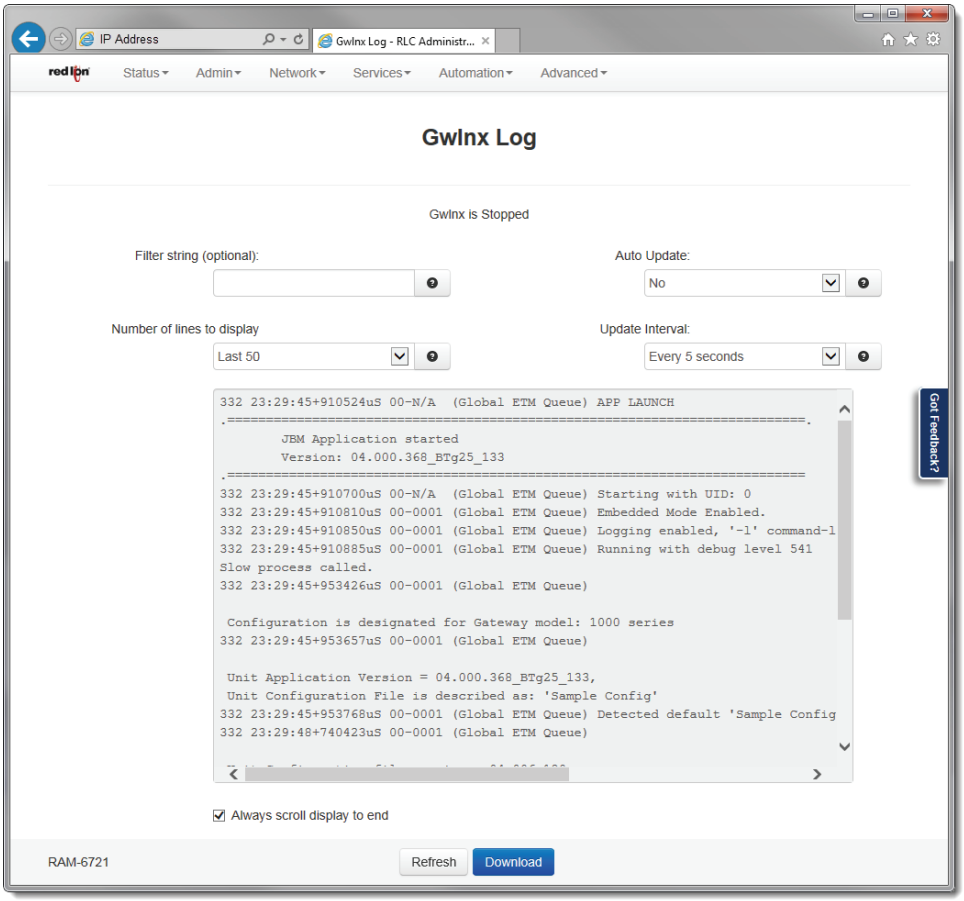
- Click on the Restart Button. This will restart the unit.

3.7.6.7 Gwnlx Log

The Gwlnx Log menu item is used to view the logfile generated by Gwlnx at startup, which provides the state of each port controller defined in the Gwlnx configuration file and logs the Send/Receive traffics for each configured port controller.



- Click on the Gwlnx Log menu item and the following dialog window will appear:


IP Address
Gwlnx Log - RLC Administr...
Status
Admin
Network
Services
Automation
Advanced
Gwlnx Log
Gwlnx is Stopped
Filter string (optional):
Auto Update:
No
Number of lines to display
Last 50
Update Interval:
Every 5 seconds
332 23:29:45+910524uS 00-N/A (Global ETM Queue) APP LAUNCH
JBM Application started
Version: 04.000.368_BTg25_133
332 23:29:45+910700uS 00-N/A (Global ETM Queue) Starting with UID: 0
332 23:29:45+910810uS 00-0001 (Global ETM Queue) Embedded Mode Enabled.
332 23:29:45+910850uS 00-0001 (Global ETM Queue) Logging enabled, '-l' command-l
332 23:29:45+910885uS 00-0001 (Global ETM Queue) Running with debug level 541
Slow process called.
332 23:29:45+953426uS 00-0001 (Global ETM Queue)
Configuration is designated for Gateway model: 1000 series
332 23:29:45+953657uS 00-0001 (Global ETM Queue)
Unit Application Version = 04.000.368_BTg25_133,
Unit Configuration File is described as: 'Sample Config'
332 23:29:45+953768uS 00-0001 (Global ETM Queue) Detected default 'Sample Config
332 23:29:48+740423uS 00-0001 (Global ETM Queue)
Always scroll display to end
RAM-6721
Refresh
Download
Got Feedback?

Filter string (optional): Enter a filter string in the space provided, only lines containing the filter value(s) will be displayed via a 'grep' style filter mechanism. Note that the filter is case sensitive.

Number of lines to display: Select the number of lines to be displayed from one of the choices in the drop-down list provided. Choices include: 50, 100, 250, 500, 1000 & 2000.

Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

Auto Update: Select Yes to enable automatic updating of the log file display, the update interval can be selected using the Select Update Interval provided immediately below this control. Manual updating is disabled while auto update is in effect. The current filter and maximum lines to be displayed will be used.

Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

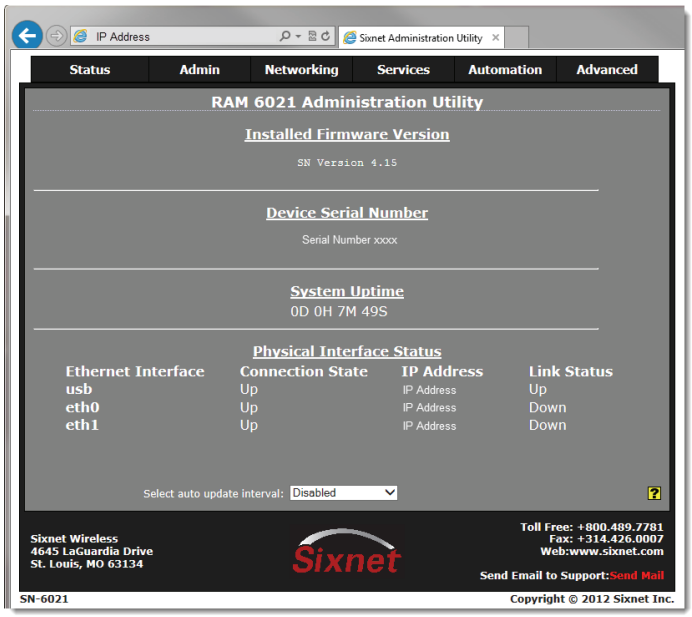
Update Interval: Select the update interval to be used when auto update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 5, 15, 30 & 60.

Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

- Click on the Download button to send the entire Gwlnx logfile “logfile.txt” to your PC download directory. Click on the Refresh button to view the latest items being logged.

3.7.7 Classic View

If you prefer the original user interface, you may revert back to it by selecting the Classic View option. The functionality is the same as in the Web User Interface documented in this manual.



Chapter 4 Red Lion Support

Technical Support

For Technical Support on all products, Red Lion provides live phone support to serve you better.

Hours are 8:00am to 5:30pm EST, Monday through Friday.

Phone: 1-877-432-9908

e-mail: support@redlion.net

Website: www.redlion.net

Customer Service

Contact the Customer Service Department for all your product requirements. The Customer Service Representatives are ready to take your orders, check product availability and order status, handle literature requests, and answer any ordering questions you may have.

Hours are 8:00am to 5pm EST, Monday through Friday.

Phone: 1-717-767-6511

email: customer.service@redlion.net

Website: www.redlion.net

Our Address

Red Lion Controls

20 Willow Springs Circle

York, PA 17406 USA

Website: www.redlion.net

Chapter 5 Compliance Statements & User Information

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates uses and can radiate radio frequency energy; and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Per FCC requirements the antenna gain including cable loss must not exceed 7.5 dBi in the Cellular band, 3 dBi in the PC-band, 5.5 dBi in the LTE Band 4, and 9 dBi in the LTE Band 17 for RF exposure purposes of 2.1091. The antenna(s) used for-this transmitter must be installed to provide a separation distance of at least 20 cm from all persons. The antenna(s) used-for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except inaccordance with FCC multi-transmitter evaluation procedures

Information to the User

If this equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

In order to meet FCC emissions limits, this equipment must be used only with cables that comply with IEEE 802.3

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

"How to Identify and Resolve Radio-TV Interference Problems".

This booklet is available from: U.S. Government Printing Office, Washington DC, 20402 Stock No. 004-000-00345-4

Canadian Compliance Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matérial brouilleur du Canada.

Chapter 6 Licensing & Warranty

Software supplied with each Red Lion product remains the exclusive property of Red Lion. Red Lion grants with each unit a perpetual license to use this software with the express limitations that the software may not be copied or used in any other product for any purpose. It may not be reverse engineered, or used for any other purpose other than in and with the computer hardware sold by Red Lion.

Statement of Limited Warranty

Red Lion, manufacturer of Red Lion products, warrants to Buyer that products, except software, manufactured by Red Lion will be free from defects in material and workmanship. Red Lion's obligation under this warranty will be limited to repairing or replacing, at Red Lion's option, the defective parts within three (3) years of the data of installation, or within three (3) years of the date of shipment from the point of manufacture, whichever is sooner. Products may be returned by Buyer only after permission has been obtained from Red Lion. Buyer will prepay all freight charges to return any products to the repair facility designated by Red Lion.

This limited warranty does not cover losses or damages which occur in shipment to or from Buyer or due to improper installation, maintenance, misuse, neglect of any cause other than ordinary commercial or industrial applications. In particular, Red Lion makes no warranties whatsoever with respect to implied warranties or merchantability or fitness for any particular purpose. All such warranties are hereby expressly disclaimed. No oral or written information or advice given by Red Lion or Red Lion's representative shall create a warranty or in any way increase the scope of this warranty.

This limited warranty is in lieu of all other warranties whether oral or written, expressed or implied. Red Lion's liability shall not exceed the price of the individual units, which are the basis of the claim. In no event shall Red Lion be liable for any loss of profits, loss of use of facilities or equipment, or other indirect, incidental or consequential damages.

Extended Warranty Program

Red Lion offers an extended warranty for the router. This program extends the original warranty on a yearly basis. In addition to extending the original warranty, the emergency replacement program is included for the cost of freight only.

The extension must be purchased before the original warranty expires. Please contact Red Lion for further information

Except for the express warranty set forth herein, Red Lion grants no warranties, either express or implied, of merchantability and fitness. The stated express warranty is in lieu of all liabilities or obligations of Red Lion for damages including but not limited to consequential damages occurring out of or in connection with the delivery, use or performance of Red Lion products.

Chapter 7 Appendices

Appendix A: RED-LION-RAM.MIB Contents

Refers to: 3.5.10 SNMP Agent: RED-LION-RAM.MIB Contents

Please note that the RAM-6021 Wired Router will not return any values for Wireless specific fields.

The following MIBs are cellular specific. It is to be noted that all of the following can be retrieved on the SN firmware version of Red Lion's routers, the A, M, and R Series routers are dependent on the cellular module/ aircard installed/inserted into the router. Some manufacturers allow for more information to be retrieved from the module/aircard than others.		
unitDescription	STRING	Router Model Name
unitSerialNumber	STRING	Serial Number of Router
unitFirmwareVer-sion	STRING	Firmware Version Number of Router
mdn	STRING	Mobile Directory Number, the actual phone number of the device.
minIMEI	STRING	Mobile Identification Number, the number given to a service plan provided by the carrier. International Mobile Equipment Ind entity, number used by the GSM network to identify valid devices.
nai	STRING	Network Access Identifier, a standard way of identifying users who request access to a network.
sipUser	INTEGER	Session Initiation Protocol, used to establish sessions between multiple parties in a location-independent manner. Typically voice sessions.
sid	INTEGER	System ID, a unique 5-digit number assigned to each carrier by the FCC.
nid	INTEGER	Network ID, used to divide SIDs into smaller areas.
prl	INTEGER	Preferred Roaming List, a list of information that resides in the memory of the module/aircard. It lists the radio frequencies the module/aircard can use in various geographic areas. The part of the list for each area is ordered by the bands the module/aircard should try to use first. Therefore it's a kind of priority list for which towers the module/aircard should use. The PRL helps determine which home-network towers to use, and also which towers belonging to other networks to use in roaming situations (areas where the home network has no coverage.) When roaming, the PRL may instruct the module/aircard to use the network with the best roaming rate for the carrier, rather than the one with the strongest signal at the moment. Since a PRL tells the module/aircard “where” to search for a signal, as carrier networks change over time, an updated PRL may be required for a module/aircard to “see” all of the coverage that it should, both with the home network and for roaming.
activated	INTEGER	Determines if the module/aircard is authorized onto the carrier's network. Values are Unknown(-1), No(0), Yes(1).

omaSupported	INTEGER	Open Mobile Alliance for Device Management (OMA DM), designed for management of small mobile devices such as mobile phones, PDAs and palm top computers. The device management is intended to support the following typical uses: **Provisioning** – Configuration of the device (including first time use), enabling and disabling features **Configuration of Device** – Allow changes to settings and parameters of the device **Software Upgrades** – Provide for new software and/or bug fixes to be loaded on the device, including applications and system software. **Fault Management** – Report errors from the device, query about status of device **Values are Unknown**(-1), No(0), Yes (1)
currentMipProfile	INTEGER	Mobile IP Profile,
esn	STRING	Electronic Serial Number, is a permanent identification number used to recognize mobile devices accessing particular telecommunications networks. The ESN is assigned and embedded into a wireless communications device by the device's manufacturer.
pesn	STRING	Pseudo ESN, a reserved ESN manufacturer code 128, which allow legacy equipment to recognize MEIDs.
meid	STRING	Mobile Equipment Identifier, 56 bits long, and like ESN's, identify the manufacturer of a mobile device as well as the serial number assigned to the device by that manufacturer.
vendor	STRING	Manufacturer of the module/aircard.
modelName	STRING	The vendor-provided model name of the module/aircard.
fwVersion	STRING	Firmware Version of the module/aircard.
hwVersion	STRING	Hardware Version of the module/aircard.
carrier	STRING	Service provider for cellular network.
lowRssi	INTEGER	Low Speed Received Signal Strength Indication
lowEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers “cleanness” in its signal to you. In other words - signal to noise ratio.
highRssi	INTEGER	High Speed Received Signal Strength Indication
highEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers “cleanness” in its signal to you. In other words - signal to noise ratio.
currentRssi	INTEGER	Current Received Signal Strength Indication
currentEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers “cleanness” in its signal to you. In other words - signal to noise ratio.
svcType	STRING	GSM, which stands for Global System for Mobile communications, reigns as the world’s most widely used cell phone technology. CDMA, or Code Division Multiple Access, uses a “spread-spectrum” technique whereby electromagnetic energy is spread to allow for a signal with a wider bandwidth. This allows multiple people on multiple cell phones to be “multiplexed” over the same channel to share a bandwidth of frequencies.
currentChannel	INTEGER	Channels are used to different frequency range network to operate on the same frequency in the same area that do not interfere with each other.
cdmaType	STRING	None, Analog, Digital - High Data Rate type, normally Digital

hdrType	STRING	Unknown, None, Rev0, RevA - The CDMA/EV-DO sub type
cdmaRoaming	STRING	Home, Roaming, Roaming - unknown. Roaming type indicator inside or outside the providers home network.
hdrRoaming	STRING	None, Roaming - SIDS Guaranteed, Roaming - SIDS Not Guaranteed. EV-DO Roaming state.
roaming	INTEGER	0, 1. 0 currently not roaming, 1 currently roaming.
currentState	INTEGER	Connecting, Dormant, Connected, Disconnected, Error, CallIncoming. Current Modem State.
speedPref	STRING	Automatic, CDMAonly, EVDOonly. What speed preference the modem is currently set to lock to.
roamPref	STRING	HomeOnly, HomePreferred - AUTO, RoamOnly, Aonly, Bonly, AutoA, AutoB, unknown. The current setting for the modem's network roaming preference.
devName	STRING	The device name as presented by the operating system.
ifName	STRING	The cellular interface name, if known, as presented by the operating system (e.g. ppp0).
txCount	INTEGER	Current Wireless PPP TX byte count since connection has been up, updated every 30 mins
rxCount	INTEGER	Current Wireless PPP RX byte count since connection has been up, updated every 30 mins
gprsState	STRING	The “state” of the GSM connection: idle, ready, standby
rxLevel	STRING	The signal level seen at the receiver measured in -dBm
servingCell	STRING	The Current Cell on which the device is camped.
rrcState	STRING	Radio Resources Control State (also called Packet Data Transfer state): idle, CELL_DCH, CELL_FACH, CELL_PCH, and URA_PCH
gsmChannel	STRING	Indicates which GSM channel or band of frequencies the device is currently connected to.
psState	STRING	Pulls CELLMODEM_PS_STATE from /var/log/wireless.cardstats
mode	STRING	Pulls CELLMODEM_MODE from /var/log/wireless.cardstats
temperature	STRING	Pulls CELLMODEM_TEMPERATURE from /var/log/wireless.cardstats
simContextApn0	STRING	Pulls CELLMODEM_SIM_CONT_APN0 from /var/log/wireless.cardstats
simContextApn1	STRING	Pulls CELLMODEM_SIM_CONT_APN1 from /var/log/wireless.cardstats
simStatus	STRING	Pulls CELLMODEM_SIM_STATUS from /var/log/wireless.cardstats
serviceDomain	STRING	Pulls CELLMODEM_SERVICE_DOMAIN from /var/log/wireless.cardstats
availServiceType	STRING	Pulls CELLMODEM_AVAIL_SERVICE_TYPE from /var/log/wireless.cardstats
wCdmaL1State	STRING	Pulls CELLMODEM_WCDMA_L1_STATE from /var/log/wireless.cardstats
mmccState	STRING	Pulls CELLMODEM_MM_CS_STATE from /var/log/wireless.cardstats
gmmPsState	STRING	Pulls CELLMODEM_GMM_PS_STATE from /var/log/wireless.cardstats
wCdmaChannel	STRING	Pulls CELLMODEM_WCDMA_CHANNEL from /var/log/wireless.cardstats
wCdmaBand	STRING	Pulls CELLMODEM_WCDMA_BAND from /var/log/wireless.cardstats
systemMode	STRING	Pulls CELLMODEM_SYSTEM_MODE from /var/log/wireless.cardstats
powerOnTime	STRING	Pulls CELLMODEM_POWERON_TIME from /var/log/wireless.cardstats
lowSpeedCsq	STRING	Pulls CELLMODEM_LOWSPEED_CSQ from /var/log/wireless.cardstats
highSpeedCsq	STRING	Pulls CELLMODEM_HIGHSPEED_CSQ from /var/log/wireless.cardstats
band	STRING	Pulls CELLMODEM_BAND from /var/log/wireless.cardstats
imei	STRING	Pulls CELLMODEM_IMEI from /var/log/wireless.cardstats
simId	STRING	Pulls CELLMODEM_SIM_ID from /var/log/wireless.cardstats